DOCKET NO.: 255234US6PCT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Satoshi KITANI, et al.
SERIAL NO.: NEW U.S. PCT APPLICATION
FILED: HEREWITH
INTERNATIONAL APPLICATION NO.: PCT/JP03/16937
INTERNATIONAL FILING DATE: December 26, 2003
FOR: SIGNAL PROCESSING SYSTEM, RECORDING METHOD, PROGRAM, RECORDING MEDIUM, REPRODUCING APPARATUS, AND INFORMATION PROCESSING APPARATUS

REQUEST FOR PRIORITY UNDER 35 U.S.C. 119 AND THE INTERNATIONAL CONVENTION

Commissioner for Patents
Alexandria, Virginia 22313

Sir:

In the matter of the above-identified application for patent, notice is hereby given that the applicant claims as priority:

COUNTRY	APPLICATION NO	DAY/MONTH/YEAR
Japan	2003-006916	15 January 2003

Certified copies of the corresponding Convention application(s) were submitted to the International Bureau in PCT Application No. PCT/JP03/16937. Receipt of the certified copy(s) by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.

Respectfully submitted,
OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Gregory J. Maier
Attorney of Record
Registration No. 25,599
Surinder Sachar
Registration No. 34,423

Customer Number
22850

(703) 413-3000
Fax No. (703) 413-2220
(OSMMN 08/03)

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　１月１５日

出願番号
Application Number: 特願２００３－００６９１６

[ST. 10/C]: ［ＪＰ２００３－００６９１６］

出願人
Applicant(s): ソニー株式会社

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

２００３年１１月　７日

特許庁長官
Commissioner,
Japan Patent Office
今井康夫

出証番号　出証特２００３－３００２３１０

【書類名】　特許願
【整理番号】　0290810006
【提出日】　平成15年 1月15日
【あて先】　特許庁長官　太田　信一郎　殿
【国際特許分類】　H04N　5/85
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
　【氏名】　木谷　聡
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
　【氏名】　村松　克美
【特許出願人】
　【識別番号】　000002185
　【氏名又は名称】　ソニー株式会社
【代理人】
　【識別番号】　100082762
　【弁理士】
　【氏名又は名称】　杉浦　正知
　【電話番号】　03-3980-0339
【選任した代理人】
　【識別番号】　100120640
　【弁理士】
　【氏名又は名称】　森　幸一
【手数料の表示】
　【予納台帳番号】　043812
　【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　0201252

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　信号処理システム、記録方法、プログラム、記録媒体、再生装置および情報処理装置

【特許請求の範囲】

【請求項１】　記録媒体固有の情報をあらかじめ備えた記録媒体から情報を読み出す再生装置と、上記再生装置が伝達手段を介して相互認証接続される情報処理装置とを備える信号処理システムであって、

上記再生装置は、

中間鍵情報に基づいてコンテンツ情報暗号化鍵を生成する最終暗号化鍵生成手段と、

上記中間鍵情報を上記伝達手段を介して上記情報処理装置へ送る第１の送信手段と、

上記コンテンツ情報暗号化鍵を上記伝達手段を介して上記情報処理装置へ送る第２の送信手段とを有し、

上記情報処理装置は、

上記コンテンツ情報暗号化鍵によりコンテンツ情報を暗号化するコンテンツ情報暗号化手段と、

上記記録媒体固有の情報に基づいて生成される記録媒体固有の鍵情報を用いて上記中間鍵情報を暗号化する中間鍵情報暗号化手段と、

暗号化された上記コンテンツ情報および暗号化された上記中間鍵情報とを上記記録媒体に記録する記録手段とを有する信号処理システム。

【請求項２】　請求項１において、

上記再生装置は、

乱数を生成する乱数生成手段を有し、

上記中間鍵情報は、

上記乱数生成手段により生成された乱数である信号処理システム。

【請求項３】　記録媒体固有の情報をあらかじめ備えた記録媒体から情報を読み出す再生装置と、上記再生装置が伝達手段を介して相互認証接続される情報処理装置とが、上記記録媒体に情報を記録する記録方法であって、

上記再生装置は、

中間鍵情報に基づいてコンテンツ情報暗号化鍵を生成する最終暗号化鍵生成ステップと、

上記中間鍵情報を上記伝達手段を介して上記情報処理装置へ送る第１の送信ステップと、

上記コンテンツ情報暗号化鍵を上記伝達手段を介して上記情報処理装置へ送る第２の送信ステップとを有し、

上記情報処理装置は、

上記コンテンツ情報暗号化鍵によりコンテンツ情報を暗号化するコンテンツ情報暗号化ステップと、

上記記録媒体固有の情報に基づいて生成される記録媒体固有の鍵情報を用いて上記中間鍵情報を暗号化する中間鍵情報暗号化ステップと、

暗号化された上記コンテンツ情報および暗号化された上記中間鍵情報とを上記記録媒体に記録する記録ステップとを有する記録方法。

【請求項４】　請求項３において、

上記再生装置は、

乱数を生成する乱数生成ステップを有し、

上記中間鍵情報は、

上記乱数生成ステップにより生成された乱数である記録方法。

【請求項５】　記録媒体固有の情報をあらかじめ備えた記録媒体から情報を読み出す再生装置と、上記再生装置が伝達手段を介して相互認証接続される情報処理装置とが、上記記録媒体に情報を記録するプログラムであって、

上記再生装置に、

中間鍵情報に基づいてコンテンツ情報暗号化鍵を生成する最終暗号化鍵生成ステップと、

上記中間鍵情報を上記伝達手段を介して上記情報処理装置へ送る第１の送信ステップと、

上記コンテンツ情報暗号化鍵を上記伝達手段を介して上記情報処理装置へ送る第２の送信ステップとを行わせ、

上記情報処理装置に、

上記コンテンツ情報暗号化鍵によりコンテンツ情報を暗号化するコンテンツ情報暗号化ステップと、

上記記録媒体固有の情報に基づいて生成される記録媒体固有の鍵情報を用いて上記中間鍵情報を暗号化する中間鍵情報暗号化ステップと、

暗号化された上記コンテンツ情報および暗号化された上記中間鍵情報とを上記記録媒体に記録する記録ステップとを行わせるプログラム。

【請求項６】　請求項５において、

上記再生装置に、

乱数を生成する乱数生成ステップを行わせ、

上記中間鍵情報は、

上記乱数生成ステップにより生成された乱数であるプログラム。

【請求項７】　記録媒体固有の情報をあらかじめ備えた記録媒体から情報を読み出す再生装置と、上記再生装置が伝達手段を介して相互認証接続される情報処理装置とが、上記記録媒体に情報を記録するプログラムを格納した記録媒体であって、

上記再生装置に、

中間鍵情報に基づいてコンテンツ情報暗号化鍵を生成する最終暗号化鍵生成ステップと、

上記中間鍵情報を上記伝達手段を介して上記情報処理装置へ送る第１の送信ステップと、

上記コンテンツ情報暗号化鍵を上記伝達手段を介して上記情報処理装置へ送る第２の送信ステップを行わせ、

上記情報処理装置に、

上記コンテンツ情報暗号化鍵によりコンテンツ情報を暗号化するコンテンツ情報暗号化ステップと、

上記記録媒体固有の情報に基づいて生成される記録媒体固有の鍵情報を用いて上記中間鍵情報を暗号化する中間鍵情報暗号化ステップと、

暗号化された上記コンテンツ情報および暗号化された上記中間鍵情報とを上記

記録媒体に記録する記録ステップとを行わせるプログラムを格納した記録媒体。

【請求項８】　請求項７において、

上記再生装置に、

乱数を生成する乱数生成ステップを行わせ、

上記中間鍵情報は、

上記乱数生成ステップにより生成された乱数であるプログラムを格納した記録媒体。

【請求項９】　記録媒体固有の情報をあらかじめ備えた記録媒体から情報を読み出し、伝達手段を介して情報処理装置と接続される再生装置であって、

中間鍵情報に基づいてコンテンツ情報暗号化鍵を生成する最終暗号化鍵生成手段と、

上記中間鍵情報を上記伝達手段を介して上記情報処理装置へ送る第１の送信手段と、

上記コンテンツ情報暗号化鍵を上記伝達手段を介して上記情報処理装置へ送る第２の送信手段とを有し、

上記コンテンツ情報暗号化鍵によりコンテンツ情報を暗号化するコンテンツ情報暗号化手段と、上記記録媒体固有の情報に基づいて生成される記録媒体固有の鍵情報を用いて上記中間鍵情報を暗号化する中間鍵情報暗号化手段と、暗号化された上記コンテンツ情報および暗号化された上記中間鍵情報とを上記記録媒体に記録する記録手段とを有する上記情報処理装置と相互認証接続される再生装置。

【請求項１０】　請求項９において、

乱数を生成する乱数生成手段を有し、

上記中間鍵情報は、

上記乱数生成手段により生成された乱数である再生装置。

【請求項１１】　記録媒体固有の情報をあらかじめ備えた記録媒体から情報を読み出す再生装置と伝達手段を介して接続される情報処理装置であって、

中間鍵情報に基づいてコンテンツ情報暗号化鍵を生成する最終暗号化鍵生成手段と、上記中間鍵情報を上記伝達手段を介して上記情報処理装置へ送る第１の送信手段と、上記コンテンツ情報暗号化鍵を上記伝達手段を介して上記情報処理装

置へ送る第２の送信手段とを有する上記再生装置と伝達手段を介して相互認証接続され、

上記コンテンツ情報暗号化鍵によりコンテンツ情報を暗号化するコンテンツ情報暗号化手段と、

上記記録媒体固有の情報に基づいて生成される記録媒体固有の鍵情報を用いて上記中間鍵情報を暗号化する中間鍵情報暗号化手段と、

暗号化された上記コンテンツ情報および暗号化された上記中間鍵情報を上記記録媒体に記録する記録手段とを有する情報処理装置。

【請求項１２】　請求項１１において、

上記再生装置は、

乱数を生成する乱数生成手段を有し、

上記中間鍵情報は、

上記乱数生成手段により生成された乱数である情報処理装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

この発明は、例えばパーソナルコンピュータと接続されたドライブによってディスクメディアに暗号化コンテンツを記録し、また、ディスクメディアから暗号化コンテンツを再生する場合に適用される信号処理システム、記録方法、プログラム、記録媒体、再生装置および情報処理装置に関する。

【０００２】

【従来の技術】

近年開発されたＤＶＤ(Digital Versatile Disc またはDigital Video Disc)等の記録媒体では、１枚の媒体に例えば映画１本分の大量のデータをディジタル情報として記録することが可能である。このように映像情報等をディジタル情報として記録することが可能となってくると不正コピーを防止して著作権の保護を図ることがますます重要となっている。

【０００３】

ＤＶＤ－Videoでは、コピープロテクション技術としてＣＳＳ(Content Scramb

ling System)が採用されている。ＣＳＳは、ＤＶＤ－ＲＯＭメディアに対する適用のみが認可されており、ＤＶＤ－Ｒ、ＤＶＤ－ＲＷ、ＤＶＤ＋Ｒ、ＤＶＤ＋ＲＷ等の記録型ＤＶＤでのＣＳＳの利用がＣＳＳ契約によって禁止されている。したがって、ＣＳＳ方式で著作権保護されたＤＶＤ－Videoの内容を記録型ＤＶＤへのまるごとコピー（ビットバイビットコピー）することは、ＣＳＳ契約上では、認められた行為ではない。

【０００４】

しかしながら、ＣＳＳの暗号方式が破られる事態が発生した。ＣＳＳの暗号化を解除してＤＶＤ－Videoの内容を簡単にハードディスクにコピーすることを可能とする「ＤｅＣＳＳ」と呼ばれるソフトウェアがインターネット上で配布された。「ＤｅＣＳＳ」が出現した背景には、本来耐タンパー化が義務付けられているはずのＣＳＳ復号用の鍵データを耐タンパー化しないまま設計された再生ソフトウェアがリバースエンジニアされて鍵データが解読されたことによって、連鎖的にＣＳＳアルゴリズム全体が解読された経緯がある。

【０００５】

ＣＳＳの後に、ＤＶＤ－Audio等のＤＶＤ－ＲＯＭの著作権保護技術であるＣＰＰＭ(Content Protection for Pre-Recorded Media)、並びに記録型ＤＶＤ、メモリカードに関する著作権保護技術ＣＰＲＭ(Content Protection for Recordable Media) が提案されている。これらの方式は、コンテンツの暗号化や管理情報の格納等に問題が生じたときに、システムを更新でき、また、データをまるごとコピーしても再生を制限できる特徴を有している。ＤＶＤに関する著作権保護の方法に関しては、下記の非特許文献１に説明され、ＣＰＲＭは、ライセンス管理者である米4C Entity,LLCが配布する下記の資料（非特許文献２）に説明されている。

【０００６】

【非特許文献１】

山田，「ＤＶＤを起点に著作権保護空間を広げる」，日経エレクトロニクス 2001.8.13,p.143-153

【０００７】

【非特許文献２】

"Content Protection for Recordable Media Specification DVD Book"、インターネット＜ＵＲＬ：http://www.4Centity.com/＞

【０００８】

【発明が解決しようとする課題】

パーソナルコンピュータ（以下、適宜ＰＣと略す）環境下では、ＰＣとドライブとが標準的インターフェースで接続されるために、標準的インターフェースの部分で秘密保持が必要なデータが知られたり、データが改ざんされるおそれがある。また、アプリケーションソフトウェアがリバースエンジニアリングされ、秘密情報が盗まれたり、改ざんされる危険がある。このような危険性は、記録再生装置が一体に構成された電子機器の場合では、生じることが少ない。

【０００９】

著作権保護技術をＰＣ上で実行されるアプリケーションプログラムへ実装する際には、その著作権保護技術の解析を防ぐため耐タンパー性を持たせるのが一般的である。しかしながら、耐タンパー性の強度を示す指標がなく、その結果、どの程度のリバースエンジニアリングへの対応を行うかは、インプレメンターの個々の判断や能力に委ねられているのが現状である。ＣＳＳの場合は、結果としてその著作権保護技術が破られてしまった。さらに、ＣＳＳの後に提案されたＣＰＰＭおよび記録型ＤＶＤに関する著作権保護技術ＣＰＲＭにおいても、既に破られているＣＳＳに新たな機能を加えたものであり、また、著作権保護技術に関わるアルゴリズムは、大部分がＰＣでの実装に依存するものであり、コンテンツプロテクションの機能が充分に強いものと言えない問題があった。すなわち、アプリケーションソフトウェアなどのリバースエンジニアリングによって、著作権保護技術に関わる秘密情報の解析により暗号方式が破られ、ディスクからのデータとしてＰＣがそのまま読み出した暗号化コンテンツが「ＤｅＣＳＳ」のような解読ソフトウェアにより復号され、平文のままのクリア・コンテンツとしてコピー制限の働かない状態で複製が繰り返されるような事態を招くことで、著作権保護が機能しなくなるという危険性があった。

【００１０】

したがって、この発明の目的は、ＰＣ環境下でも著作権保護技術の安全性を確保することができる信号処理システム、記録方法、プログラム、記録媒体、再生装置および情報処理装置を提供することにある。

【００１１】

【課題を解決するための手段】

上述した課題を解決するために、請求項１の発明は、記録媒体固有の情報をあらかじめ備えた記録媒体から情報を読み出す再生装置と、再生装置が伝達手段を介して相互認証接続される情報処理装置とを備える信号処理システムであって、

再生装置は、

中間鍵情報に基づいてコンテンツ情報暗号化鍵を生成する最終暗号化鍵生成手段と、

中間鍵情報を伝達手段を介して情報処理装置へ送る第１の送信手段と、

コンテンツ情報暗号化鍵を伝達手段を介して情報処理装置へ送る第２の送信手段とを有し、

情報処理装置は、

コンテンツ情報暗号化鍵によりコンテンツ情報を暗号化するコンテンツ情報暗号化手段と、

記録媒体固有の情報に基づいて生成される記録媒体固有の鍵情報を用いて中間鍵情報を暗号化する中間鍵情報暗号化手段と、

暗号化されたコンテンツ情報および暗号化された中間鍵情報とを記録媒体に記録する記録手段とを有する信号処理システムである。

【００１２】

請求項３の発明は、記録媒体固有の情報をあらかじめ備えた記録媒体から情報を読み出す再生装置と、再生装置が伝達手段を介して相互認証接続される情報処理装置とが、記録媒体に情報を記録する記録方法であって、

再生装置は、

中間鍵情報に基づいてコンテンツ情報暗号化鍵を生成する最終暗号化鍵生成ステップと、

中間鍵情報を伝達手段を介して情報処理装置へ送る第１の送信ステップと、

コンテンツ情報暗号化鍵を伝達手段を介して情報処理装置へ送る第２の送信ステップとを有し、

情報処理装置は、

コンテンツ情報暗号化鍵によりコンテンツ情報を暗号化するコンテンツ情報暗号化ステップと、

記録媒体固有の情報に基づいて生成される記録媒体固有の鍵情報を用いて中間鍵情報を暗号化する中間鍵情報暗号化ステップと、

暗号化されたコンテンツ情報および暗号化された中間鍵情報とを記録媒体に記録する記録ステップとを有する記録方法である。

【００１３】

請求項５の発明は、記録媒体固有の情報をあらかじめ備えた記録媒体から情報を読み出す再生装置と、再生装置が伝達手段を介して相互認証接続される情報処理装置とが、記録媒体に情報を記録するプログラムであって、

再生装置に、

中間鍵情報に基づいてコンテンツ情報暗号化鍵を生成する最終暗号化鍵生成ステップと、

中間鍵情報を伝達手段を介して情報処理装置へ送る第１の送信ステップと、

コンテンツ情報暗号化鍵を伝達手段を介して情報処理装置へ送る第２の送信ステップとを行わせ、

情報処理装置に、

コンテンツ情報暗号化鍵によりコンテンツ情報を暗号化するコンテンツ情報暗号化ステップと、

記録媒体固有の情報に基づいて生成される記録媒体固有の鍵情報を用いて中間鍵情報を暗号化する中間鍵情報暗号化ステップと、

暗号化されたコンテンツ情報および暗号化された中間鍵情報とを記録媒体に記録する記録ステップとを行わせるプログラムである。

【００１４】

請求項７の発明は、記録媒体固有の情報をあらかじめ備えた記録媒体から情報を読み出す再生装置と、再生装置が伝達手段を介して相互認証接続される情報処

理装置とが、記録媒体に情報を記録するプログラムを格納した記録媒体であって、

再生装置に、

中間鍵情報に基づいてコンテンツ情報暗号化鍵を生成する最終暗号化鍵生成ステップと、

中間鍵情報を伝達手段を介して情報処理装置へ送る第１の送信ステップと、

コンテンツ情報暗号化鍵を伝達手段を介して情報処理装置へ送る第２の送信ステップを行わせ、

情報処理装置に、

コンテンツ情報暗号化鍵によりコンテンツ情報を暗号化するコンテンツ情報暗号化ステップと、

記録媒体固有の情報に基づいて生成される記録媒体固有の鍵情報を用いて中間鍵情報を暗号化する中間鍵情報暗号化ステップと、

暗号化されたコンテンツ情報および暗号化された中間鍵情報とを記録媒体に記録する記録ステップとを行わせるプログラムを格納した記録媒体である。

【００１５】

請求項９の発明は、記録媒体固有の情報をあらかじめ備えた記録媒体から情報を読み出し、伝達手段を介して情報処理装置と接続される再生装置であって、

中間鍵情報に基づいてコンテンツ情報暗号化鍵を生成する最終暗号化鍵生成手段と、

中間鍵情報を伝達手段を介して情報処理装置へ送る第１の送信手段と、

コンテンツ情報暗号化鍵を伝達手段を介して情報処理装置へ送る第２の送信手段とを有し、

コンテンツ情報暗号化鍵によりコンテンツ情報を暗号化するコンテンツ情報暗号化手段と、記録媒体固有の情報に基づいて生成される記録媒体固有の鍵情報を用いて中間鍵情報を暗号化する中間鍵情報暗号化手段と、暗号化されたコンテンツ情報および暗号化された中間鍵情報とを記録媒体に記録する記録手段とを有する情報処理装置と相互認証接続される再生装置である。

【００１６】

請求項１１の発明は、記録媒体固有の情報をあらかじめ備えた記録媒体から情報を読み出す再生装置と伝達手段を介して接続される情報処理装置であって、

中間鍵情報に基づいてコンテンツ情報暗号化鍵を生成する最終暗号化鍵生成手段と、中間鍵情報を伝達手段を介して情報処理装置へ送る第１の送信手段と、コンテンツ情報暗号化鍵を伝達手段を介して情報処理装置へ送る第２の送信手段とを有する再生装置と伝達手段を介して相互認証接続され、

コンテンツ情報暗号化鍵によりコンテンツ情報を暗号化するコンテンツ情報暗号化手段と、

記録媒体固有の情報に基づいて生成される記録媒体固有の鍵情報を用いて中間鍵情報を暗号化する中間鍵情報暗号化手段と、

暗号化されたコンテンツ情報および暗号化された中間鍵情報を記録媒体に記録する記録手段とを有する情報処理装置である。

【００１７】

この発明では、再生装置側でコンテンツキーを生成し、情報処理装置側でコンテンツキーによってコンテンツを暗号化している。このように著作権保護のための鍵情報の生成を再生装置で行うので、ハードウエア構成でコンテンツキーを生成することが可能となり、耐タンパー性を高めることができる。また、再生装置において、乱数を生成し、乱数を中間鍵とするので、再生装置において、真正乱数またはそれに近い乱数をハードウエア例えばＬＳＩによって発生することができ、生成した乱数を固定値への置き換えを困難とすることができる。このように、この発明では、情報処理装置にインストールされるアプリケーションソフトウェアは、著作権保護技術に関する秘密情報の全てを持つ必要がなくなる。それによって、ソフトウェアのリバースエンジニアリングによる解析に対する耐性を持つことができ、著作権保護技術の安全性を確保することができる。

【００１８】

また、電子機器固有の情報としてのデバイスキーを記録再生装置が持つことによって、記録再生装置自身をリボークすることが可能となる。さらに、この発明では、情報処理装置におけるコンテンツキーを計算するのに必要とされる乱数情報が記録再生装置内の例えばＬＳＩによって生成できるので、ＰＣ内でソフトウ

ェアによって乱数を生成するのと比較して、真正または真正乱数に近い乱数を生成することができる。したがって、乱数が固定値に置き換えられる、等のおそれを少なくできる。

【００１９】

【発明の実施の形態】

この発明の一実施形態の説明に先立って、本明細書の特許請求の範囲において使用される用語と実施の形態中で使用される用語との対応関係について以下に説明する。

【００２０】

記録媒体：メディア例えばディスク、再生装置：ドライブ、情報処理装置：ホスト、伝達手段：ドライブーホストインターフェース、信号処理システム：メディアを再生するドライブとホストとがドライブーホストインターフェースを介して接続されるシステムである。第１の送信手段：ドライブ側からセッションキーを共通鍵とした共通鍵暗号方式で情報をホスト側に送る手段、第２の送信手段：逆にホスト側からセッションキーを共通鍵として情報をドライブ側に送る手段のことである。

【００２１】

コンテンツ情報：メディアに記録されている情報または記録すべき情報をコンテンツ情報としている。記録媒体固有の情報：メディアＩＤである。乱数を生成する乱数生成手段：乱数発生器（ＲＮＧ：Random Number Generator)である。記録媒体固有の鍵情報：メディアユニークキー、中間鍵情報：タイトルキーである。コンテンツ情報暗号化鍵：コンテンツキー（記録時に使われるコンテンツキーをコンテンツ情報暗号化鍵とし、再生時に使われるコンテンツキーをコンテンツ情報復号鍵としている。）

【００２２】

次に、この発明の理解の容易のために、最初に図１を参照して著作権保護技術例えばＤＶＤ用ＣＰＲＭのアーキテクチャについて説明する。図１において、参照符号１が例えばＣＰＲＭ規格に準拠したＤＶＤ－Ｒ／ＲＷ、ＤＶＤ－ＲＡＭ等の記録型ＤＶＤメディアを示し、参照符号２が例えばＣＰＲＭ規格に準拠したレ

コーダを示し、参照符号３が例えばＣＰＲＭ規格に準拠したプレーヤを示す。レコーダ２およびプレーヤ３は、機器またはアプリケーションソフトウェアである。

【００２３】

未記録ディスクの状態において、ＤＶＤメディア１の最内周側のリードインエリアのＢＣＡ(Burst Cutting Area)またはＮＢＣＡ(Narrow Burst Cutting Area)と称されるエリアには、メディアＩＤ１１が記録され、リードインエリアのエンボスまたはプリ記録データゾーンには、メディアキーブロック（以下、ＭＫＢと適宜略す）１２が予め記録されている。メディアＩＤ１１は、個々のメディア単位例えばディスク１枚毎に異なる番号であり、メディアの製造者コードとシリアル番号から構成される。メディアＩＤ１１は、メディアキーを個々のメディアで異なるメディアユニークキーへ変換する際に必要となる。メディアキーブロックＭＫＢは、メディアキーの導出、並びに機器のリボケーション（無効化）を実現するための鍵束である。これらのメディアＩＤおよびメディアキーブロックは、記録媒体固有の第１の情報である。

【００２４】

ディスク１の書き換えまたは追記可能なデータ領域には、コンテンツキーで暗号化された暗号化コンテンツ１３が記録される。暗号化方式としては、Ｃ２(Cryptomeria Ciphering)が使用される。

【００２５】

ＤＶＤメディア１には、暗号化タイトルキー１４およびＣＣＩ(Copy Control Information)１５が記録される。暗号化タイトルキー１４は、暗号化されたタイトルキー情報であり、タイトルキー情報は、タイトル毎に付加される鍵情報である。ＣＣＩは、コピーノーモア、コピーワンス、コピーフリー等のコピー制御情報である。

【００２６】

レコーダ２は、デバイスキー２１、プロセスＭＫＢ２２、Ｃ２＿Ｇ２３、乱数発生器２４、Ｃ２＿Ｅ２５、Ｃ２＿Ｇ２６およびＣ２＿ＥＣＢＣ２７の構成要素を有する。プレーヤ３は、デバイスキー３１、プロセスＭＫＢ３２、Ｃ２＿Ｇ３

３、Ｃ２＿Ｄ３５、Ｃ２＿Ｇ３６およびＣ２＿ＤＣＢＣ３７の構成要素を有する。Ｃ２＿Ｇ２３および３３は、それぞれメディアＩＤとメディアキーとからメディアユニークキーを演算するブロックである。Ｃ２＿Ｇ２６および３６は、それぞれＣＣＩとタイトルキーとからコンテンツキーを演算するブロックである。

【００２７】

デバイスキー２１、３１は、個々の装置メーカ、またはアプリケーションソフトウェアベンダー毎に発行された識別番号である。デバイスキーは、ライセンス管理者によって正当な電子機器またはアプリケーションソフトウェアにのみ与えられる当該電子機器またはアプリケーションソフトウェア固有の情報である。ＤＶＤメディア１から再生されたＭＫＢ１２とデバイスキー２１とがプロセスＭＫＢ２２において演算されることによって、リボケーションされたかどうかの判別ができる。レコーダ２におけるのと同様に、プレーヤ３においても、ＭＫＢ１２とデバイスキー３１とがプロセスＭＫＢ３２において演算され、リボケーションされたかどうかの判別がなされる。

【００２８】

さらに、プロセスＭＫＢ２２、３２のそれぞれにおいて、ＭＫＢ１２とデバイスキー２１、３１からメディアキーが算出される。ＭＫＢ１２の中にレコーダ２またはプレーヤ３のデバイスキーが入っておらず、演算された結果が予め決められたある値例えばゼロの値と一致した場合、そのデバイスキーを持つレコーダ２またはプレーヤ３が正当なものでないと判断される。すなわち、そのようなレコーダ２またはプレーヤ３がリボケーションされる。

【００２９】

Ｃ２＿Ｇ２３、３３は、それぞれ、メディアキーとメディアＩＤとを演算し、メディアユニークキーを導出する処理である。

【００３０】

乱数発生器（ＲＮＧ：Random Number Generator）２４は、タイトルキーの生成に利用される。乱数発生器２４からのタイトルキーがＣ２＿Ｅ２５に入力され、タイトルキーがメディアユニークキーで暗号化される。暗号化タイトルキー１４がＤＶＤメディア１に記録される。

【００３１】

プレーヤ３では、ＤＶＤメディア１から再生された暗号化タイトルキー１４とメディアユニークキーとがＣ２＿Ｄ３５に供給され、暗号化タイトルキーがメディアユニークキーで復号され、タイトルキーが得られる。

【００３２】

レコーダ２においては、ＣＣＩとタイトルキーとがＣ２＿Ｇ２６に供給され、コンテンツキーが導出される。コンテンツキーがＣ２＿ＥＣＢＣ２７に供給され、コンテンツキーを鍵としてコンテンツが暗号化される。暗号化コンテンツ１３がＤＶＤメディア１に記録される。

【００３３】

プレーヤ３においては、ＣＣＩとタイトルキーとがＣ２＿Ｇ３６に供給され、コンテンツキーが導出される。コンテンツキーがＣ２＿ＥＣＢＣ３７に供給され、ＤＶＤメディア１から再生された暗号化コンテンツ１３がコンテンツキーを鍵として復号される。

【００３４】

図１の構成において、レコーダ２による記録の手順について説明する。レコーダ２は、ＤＶＤメディア１からＭＫＢ１２を読み出し、プロセスＭＫＢ２２によってデバイスキー２１とＭＫＢ１２とを演算し、メディアキーを計算する。演算結果が予め定められた値を示すならば、デバイスキー２１（レコーダ２の機器またはアプリケーション）がＭＫＢによってリボークされたと判定され、レコーダ２は、以後の処理を中断し、ＤＶＤメディア１への記録を禁止する。若し、メディアキーの値が予め定められた値以外であれば、処理を継続する。

【００３５】

次に、レコーダ２は、ＤＶＤメディア１からメディアＩＤ１１を読み、メディアキーと共にメディアＩＤをＣ２＿Ｇ２３に入力しメディア毎に異なるメディアユニークキーが演算される。乱数発生器２４で発生させたタイトルキーがＣ２＿Ｅ２５で暗号化され、暗号化タイトルキー１４としてＤＶＤメディア１に記録される。また、タイトルキーとコンテンツのＣＣＩ情報がＣ２＿Ｇ２６で演算され、コンテンツキーが導出される。コンテンツキーでコンテンツをＣ２＿ＥＣＢＣ

２７で暗号化し、ＤＶＤメディア１上に暗号化コンテンツ１３としてＣＣＩ１５と共に記録する。

【００３６】

プレーヤ３による再生の手順について説明する。最初にＭＫＢ１２をＤＶＤメディア１から読み出し、デバイスキー３１とＭＫＢ１２を演算し、リボケーションの確認がなされる。デバイスキー３１、すなわち、プレーヤ３の機器またはアプリケーションがリボークされない場合には、メディアＩＤを使用してメディアユニークキーが演算され、読み出された暗号化タイトルキー１４とメディアユニークキーからタイトルキーが演算される。タイトルキーとＣＣＩ１５とがＣ２＿Ｇ３６に入力され、コンテンツキーが導出される。コンテンツキーがＣ２＿ＤＣＢＣ３７に入力され、コンテンツキーを鍵として、ＤＶＤメディア１から再生された暗号化コンテンツ１３に対してＣ２＿ＤＣＢＣ３７の演算が施される。その結果、暗号化コンテンツ１３が復号される。

【００３７】

このように、コンテンツの復号に必要なコンテンツキーを得るためには、ＤＶＤメディアの１枚毎に異なるメディアＩＤが必要となるので、たとえメディア上の暗号化コンテンツが忠実に他のメディアにコピーされても、他のメディアのメディアＩＤがオリジナルのメディアＩＤと異なるために、コピーされたコンテンツを復号することができず、コンテンツの著作権を保護することができる。

【００３８】

上述した図１の構成は、記録再生機器として構成されたものである。この発明は、ＤＶＤメディア１に対するコンテンツ保護処理をＰＣ環境下で扱う場合に適用される。図２を参照して現行の方式によるＰＣとドライブの役割分担を示す。図２において、参照符号４が上述したＣＰＲＭ規格に準拠したＤＶＤメディア１を記録および再生する記録再生装置としてのＤＶＤドライブを示す。

【００３９】

参照符号５がデータ処理装置としてのホスト例えばＰＣを示す。ホスト５は、ＤＶＤメディア１に記録可能で、ＤＶＤメディア１から再生可能なコンテンツを扱うことができ、且つＤＶＤドライブ４と接続されてデータ交換が可能な装置ま

たはアプリケーションソフトウェアである。例えばＰＣに対してアプリケーションソフトウェアがインストールされることによってホスト５が構成される。

【００４０】

ＤＶＤドライブ４とホスト５との間がインターフェース４ａで接続されている。インターフェース４ａは、ＡＴＡＰＩ(AT Attachment with Packet Interface)，ＳＣＳＩ(Small Computer System Interface)，ＵＳＢ(Universal Serial Bus)，ＩＥＥＥ(Institute of Electrical and Electronics Engineers)１３９４等である。

【００４１】

ＤＶＤメディア１には、メディアＩＤ１１、メディアキーブロック１２およびＡＣＣ(Authentication Control Code)が予め記録されている。ＡＣＣは、ＤＶＤドライブ４とホスト５との間の認証がＤＶＤメディア１によって異なるようにするために予めＤＶＤメディア１に記録されたデータである。

【００４２】

ＤＶＤドライブ４は、ＡＣＣ１６をＤＶＤメディア１から読み出す。ＤＶＤメディア１から読み出されたＡＣＣ１６がＤＶＤドライブ４のＡＫＥ(Authentication and Key Exchange)４１に入力されると共に、ホスト５へ転送される。ホスト５は、受け取ったＡＣＣをＡＫＥ５１に入力する。ＡＫＥ４１および５１は、乱数データを交換し、この交換した乱数とＡＣＣの値とから認証動作の度に異なる値となる共通のセッションキー（図２の構成においてはバスキーと称する）を生成する。

【００４３】

バスキーがＭＡＣ(Message Authentication Code)演算ブロック４２および５２にそれぞれ供給される。ＭＡＣ演算ブロック４２および５２は、ＡＫＥ４１および５１でそれぞれ得られたバスキーをパラメータとして、メディアＩＤおよびメディアキーブロック１２のＭＡＣを計算するプロセスである。ＭＫＢとメディアＩＤの完全性(integrity)をホスト５が確認するために利用される。

【００４４】

ＭＡＣ４２および５２によってそれぞれ計算されたＭＡＣがホスト５の比較５

３において比較され、両者の値が一致するかどうかが判定される。これらのＭＡＣの値が一致すれば、ＭＫＢとメディアＩＤの完全性が確認されたことになる。比較出力でスイッチＳＷ１が制御される。

【００４５】

スイッチＳＷ１は、ＤＶＤドライブ４のＤＶＤメディア１の記録または再生経路と、ホスト５の暗号化／（または）復号モジュール５４との間の信号路をＯＮ／ＯＦＦするものとして示されている。なお、スイッチＳＷ１は、信号路のＯＮ／ＯＦＦを行うものとして示されているが、より実際には、ＯＮの場合にホスト５の処理が継続し、ＯＦＦの場合にホスト５の処理が停止することを表している。暗号化／復号モジュール５４は、メディアユニークキーと暗号化タイトルキーとＣＣＩとからコンテンツキーを算出し、コンテンツキーを鍵としてコンテンツを暗号化コンテンツ１３へ暗号化し、またはコンテンツキーを鍵として暗号化コンテンツ１３を復号する演算ブロックである。

【００４６】

メディアユニークキー演算ブロック５５は、ＭＫＢ１２とメディアＩＤとデバイスキー５６とからメディアユニークキーを演算する演算ブロックである。すなわち、図１に示すレコーダまたはプレーヤと同様に、デバイスキーとＭＫＢ１２とからメディアキーが演算され、さらに、メディアキーとメディアＩＤ１１とからメディアユニークキーが演算される。メディアキーが所定の値となった場合には、その電子機器またはアプリケーションソフトウェアが正当なものではないと判断され、リボークされる。したがって、メディアユニークキー演算ブロック５５は、リボケーションを行うリボーク処理部としての機能も有する。

【００４７】

記録時に、比較５３によって完全性が確認された場合には、スイッチＳＷ１がＯＮされ、暗号化／復号モジュール５４からスイッチＳＷ１を通じてドライブ４に対して、暗号化コンテンツ１３、暗号化タイトルキー１４およびＣＣＩ１５が供給され、ＤＶＤメディア１に対してそれぞれ記録される。再生時に、比較５３によって完全性が確認された場合には、スイッチＳＷ１がＯＮされ、ＤＶＤメディア１からそれぞれ再生された暗号化コンテンツ１３、暗号化タイトルキー１４

およびＣＣＩ１５がスイッチＳＷ１を通じてホスト５の暗号化／復号モジュール５４に対して供給され、暗号化コンテンツが復号される。

【００４８】

図３は、図２に示す現行のＰＣ環境下のＤＶＤメディアを利用するシステムにおいて、ＤＶＤメディア１と、ＤＶＤドライブ４と、ホスト５との間の信号の授受の手順を示す。ホスト５がＤＶＤドライブ４に対してコマンドを送り、ＤＶＤドライブ４がコマンドに応答した動作を行う。

【００４９】

最初に、ホスト５からの要求に応じてＤＶＤメディア１上のＡＣＣがシークされ、読み出される（ステップＳ１）。次のステップＳ２において、読み出されたＡＣＣがＡＫＥ４１に入力されると共に、ホスト５へ転送され、ホスト５では、受け取ったＡＣＣがＡＫＥ５１へ入力される。ＡＫＥ４１および５１は、乱数データを交換し、この交換した乱数とＡＣＣ１６の値から認証動作の度に異なる値となるセッションキーとしてのバスキーを生成し、バスキーをＤＶＤドライブ４とホスト５が共有する。相互認証が成立しなかった場合では、処理が中断する。

【００５０】

認証動作は、電源のＯＮ後のディスク検出時並びにディスクの交換時には、必ず行われる。また、記録ボタンを押して記録動作を行う場合、並びに再生ボタンを押して再生動作を行う場合に、認証動作を行うようにしても良い。一例として、記録ボタンまたは再生ボタンを押した時に、認証がなされる。

【００５１】

認証が成功すると、次に、ステップＳ３において、ホスト５がＤＶＤドライブ４に対して、ＤＶＤメディア１からのＭＫＢ（メディアキーブロック）パック＃０の読み出しを要求する。ＭＫＢは、パック０～パック１５の１６セクタが１２回繰り返してリードインエリアに記録されている。パック単位で、エラー訂正符号化がなされている。

【００５２】

ＤＶＤドライブ４がステップＳ４においてＭＫＢのパック＃０を読みに行き、ステップＳ５において、パック＃０が読み出される。ＤＶＤドライブ４は、モデ

ィファイドＭＫＢをホスト５へ戻す（ステップＳ６）。すなわち、ＭＫＢを読み出す際に、バスキーをパラメータとしてＭＡＣ値を計算し、ＭＫＢに対してＭＡＣ値を付加してホスト５へデータを転送する。パック＃０以外の残りのＭＫＢパックの要求と、ＤＶＤドライブ４の読み出し動作と、モディファイドＭＫＢパックの転送動作とがＭＫＢのパックがなくなるまで、例えばパック＃１５が読み出され、ホスト５へ転送されるまで、ステップＳ７およびＳ８によって繰り返しなされる。

【００５３】

次に、ホスト５がＤＶＤドライブ４に対してメディアＩＤを要求する。ＤＶＤドライブ４がＤＶＤメディア１に記録されているメディアＩＤを読みに行き、ステップＳ１１において、メディアＩＤが読み出される。ＤＶＤドライブ４は、メディアＩＤを読み出す際に、バスキーをパラメータとしてそのＭＡＣ値を計算し、ステップＳ１２において、読み出されたメディアＩＤに対してＭＡＣ値ｍ１を付加してホスト５へデータを転送する。

【００５４】

ホスト５では、ＤＶＤドライブ４から受け取ったＭＫＢ１２およびメディアＩＤ１１からバスキーをパラメータとして再度ＭＡＣ値を計算し、計算したＭＡＣ値とＤＶＤドライブ４から受け取ったＭＡＣ値とを比較５３で比較し、両者が一致したならば、正しいＭＫＢおよびメディアＩＤを受け取ったと判定して、スイッチＳＷ１をＯＮに設定して処理を先に進める。逆に両者が一致しなかったならば、ＭＫＢおよびメディアＩＤが改ざんされたものと判定して、スイッチＳＷ１をＯＦＦに設定して処理を中断する。

【００５５】

ステップＳ１３において、ホスト５がＤＶＤドライブ４に対して暗号化コンテンツを要求し、ステップＳ１４において、ＤＶＤドライブ４が暗号化コンテンツを読み出し、ステップＳ１３において、読み出した暗号化コンテンツがホスト５に転送される。ホスト５のメディアユニークキー演算ブロック５５では、デバイスキー５６とＭＫＢ１２とメディアＩＤ１１とによってメディアユニークキーが計算される。そして、メディアユニークキーが暗号化／復号モジュール５４に供

給され、暗号化タイトルキー１４、ＣＣＩ１５からコンテンツキーが求められ、コンテンツキーを鍵としてＤＶＤメディア１から読み出された暗号化コンテンツが復号され、また、ＤＶＤメディア１に対して記録されるコンテンツが暗号化される。

【００５６】

図４のフローチャートにおいて、ステップＳＴ１は、ＭＡＣ演算ブロック４２でバスキーをパラメータとして求められたＭＡＣ計算値と、ＭＡＣ演算ブロック５３でバスキーをパラメータとして求められたＭＡＣ計算値とを比較するステップである。両者が一致すれば、スイッチＳＷ１がステップＳＴ２においてＯＮとされ、両者が一致しない場合では、スイッチＳＷ１がステップＳＴ３においてＯＦＦとされ、処理が停止する。

【００５７】

上述したＣＰＲＭでは、ＤＶＤ－Videoの著作権保護技術であるＣＳＳと同じバスキー生成方法を採用している。ＣＳＳ認証方式の内容は、本来秘密であるべき情報であるが、既に解析され一般ユーザーが入手可能なＣＳＳライセンス管理団体であるDVD-CCAの許諾を得ていないフリーソフトウェアによって動作させることが可能となっている。また、コンテンツプロテクション処理は、ホスト側でなされる、すなわち、リボケーション判定、メディアキー取得、メディアユニークキー導出、タイトルキー生成・導出からコンテンツキー導出およびコンテンツ暗号化・復号の全てがホスト側の処理であることから、著作権保護技術としての信頼性が低下している。

【００５８】

以下に述べるこの発明の一実施形態では、かかる問題点を解決するものである。一実施形態では、ＰＣ環境下でのコンテンツプロテクション処理におけるタイトルキー導出に関わる構成をドライブ内部に持ち、ＰＣとの相互認証を経てタイトルキーおよびコンテンツキーをＰＣに送信するものである。

【００５９】

図５は、一実施形態における相互認証の構成を示すブロック図であり、図６は、ドライブ側の処理の流れを示すフローチャートであり、図７は、ホスト側の処

理の流れを示すフローチャートである。以下の説明において、参照符号１０１がメディア例えば光ディスクを示し、参照符号１０２がメディアのドライブを示し、参照符号１０３がドライブ１０２とドライブーホストインターフェース１０４を介して接続されたホストを示す。メディア１０１は、上述したＤＶＤメディアと同様の情報が予め記録されているものである。メディア１０１は、記録可能なものに限らず、読み出し専用のものでも良い。ホスト１０３がドライブ１０２に対して所定のコマンドを送り、その動作を制御する。使用するコマンドは、上述した非特許文献２に記載されているコマンド並びにコマンドを拡張したもの、および、メディア１０１からコンテンツをセクタ・データとして読み出すためのＲＥＡＤコマンド、メディア１０１へコンテンツをセクタ・データとして書き込むためのＷＲＩＴＥコマンドである。

【００６０】

ドライブ１０２は、ドライブのデバイスキー１２１を有し、ホスト１０３がホストのデバイスキー１３１を有している。デバイスキー１２１は、多くの場合にＬＳＩ(Large Scale Integrated Circuit：大規模集積回路)内部に配置され、外部から読み出すことができないようセキュアに記憶される。デバイスキー１３１は、ソフトウェアプログラム内にセキュアに記憶される場合と、ハードウェアとしてセキュアに記憶される場合とがある。また、ドライブ１０２がメディア１０１を扱う正当なドライブとなるためには、一実施形態のように、デバイスキーのような著作権保護技術に関する秘密情報を必要とするので、正規のライセンスを受けずに正規品になりすますようなクローン・ドライブの作成を防止できる効果がある。

【００６１】

図５に示すように、ドライブ１０２には、ＭＫＢとデバイスキー１２１とが入力され、ドライブのデバイスキーがリボケーションされたかどうかを判定するプロセスＭＫＢ１２２が備えられている。ホスト１０３にも同様に、プロセスＭＫＢ１３２が備えられている。リボケーションされない場合に、プロセスＭＫＢ１２２および１３２からそれぞれメディアキーＫｍが出力される。リボーク判定処理がなされ、メディアキーＫｍが得られてから認証処理がなされる。

【００６２】

参照符号１２３、１２４および１２５は、メディアキーＫｍをパラメータとしてＭＡＣ値を計算するＭＡＣ演算ブロックをそれぞれ示す。また、参照符号１２６、１２７および１２８は、乱数発生器（ＲＮＧ：Random Number Generator)をそれぞれ示す。乱数発生器１２６が乱数Ｒalを生成し、乱数発生器１２７が乱数Ｒa2を生成し、乱数発生器１２８が乱数Ｒa3を生成する。乱数発生器１２６、１２７、１２８は、例えばＬＳＩの構成の乱数発生器であり、ソフトウェアにより乱数を発生する方法と比較してより真正乱数に近い乱数を発生することができる。乱数発生器を共通のハードウエアとしても良いが、乱数Ｒal、Ｒa2、Ｒa3は、互いに独立したものである。

【００６３】

ホスト１０３に、メディアキーＫｍをパラメータとしてＭＡＣ値を計算するＭＡＣ演算ブロック１３３、１３４および１３５と、乱数発生器１３６、１３７および１３８が備えられている。乱数発生器１３６が乱数Ｒblを生成し、乱数発生器１３７が乱数Ｒb2を生成し、乱数発生器１３８が乱数Ｒb3を生成する。乱数発生器１３６、１３７、１３８は、通常はソフトウェアによって乱数を発生するものであるが、ハードウェアによる乱数が利用できる場合にはこれを用いても良い。

【００６４】

ドライブ１０２において生成された乱数とホスト１０３において生成された乱数とが交換される。すなわち、乱数Ｒalおよび乱数ＲblがＭＡＣ演算ブロック１２３および１３３に入力され、乱数Ｒa2および乱数Ｒb2がＭＡＣ演算ブロック１２４および１３４に入力され、乱数Ｒa3および乱数Ｒb3がＭＡＣ演算ブロック１２５および１３５に入力される。

【００６５】

ドライブ１０２のＭＡＣ演算ブロック１２３が演算したＭＡＣ値と、ホスト１０３のＭＡＣ演算ブロック１３３が演算したＭＡＣ値とがホスト１０３内の比較１３９において比較され、二つの値が同一か否かが判定される。ここでのＭＡＣ値は、eKm(Ral‖Rbl)と表記される。ｅＫｍ（）は、メディアキーＫｍを鍵とし

て括弧内のデータを暗号化することを表している。Ral‖Rblの記号は、左側に乱数Ralを配し、右側に乱数Rblを配するように、二つの乱数を結合することを表している。比較の結果、二つの値が同一と判定されると、ホスト１０３によるドライブ１０２の認証が成功したことになり、そうでない場合には、この認証が失敗したことになる。

【００６６】

ホスト１０３のＭＡＣ演算ブロック１３４が演算したＭＡＣ値と、ドライブ１０２のＭＡＣ演算ブロック１２４が演算したＭＡＣ値とがドライブ１０２内の比較１２９において比較され、二つの値が同一か否かが判定される。ここでのＭＡＣ値は、eKm(Rb2‖Ra2)と表記される。比較の結果、二つの値が同一と判定されると、ドライブ１０２によるホスト１０３の認証が成功したことになり、そうでない場合には、この認証が失敗したことになる。

【００６７】

かかる相互認証において、比較１３９および１２９の両者において、ＭＡＣ値が同一と判定され、ドライブ１０２およびホスト１０３の両者の正当性が確認されると、すなわち、相互認証が成功すると、ＭＡＣ演算ブロック１２５および１３５によって、共通のセッションキーeKm(Ra3‖Rb3)がそれぞれ生成される。

【００６８】

さらに、上述した相互認証の処理の流れを図６および図７のフローチャートを参照して説明する。最初に、図７のステップＳＴ２０において、ホスト１０３がドライブ１０２に対して、コマンドREPORT KEYを発行し、ＭＫＢの転送を要求する。図６のステップＳＴ１０において、ドライブ１０２がメディア１０１からＭＫＢ１１２を読み出して、ホスト１０３へ転送する。

【００６９】

次に、ドライブ１０２がステップＳＴ１１において、プロセスＭＫＢ１２２によってメディアキーＫｍを計算し、ホスト１０３がステップＳＴ２１において、プロセスＭＫＢ１３２によってメディアキーＫｍを計算する。この計算の過程でそれぞれが内蔵するデバイスキー１２１および１３１がリボケーションの対象とされているか否かが自分自身によって確認される（図６中のステップＳＴ１２、

図７中のステップＳＴ２２）。

【００７０】

ドライブ１０２およびホスト１０３のそれぞれは、リボケーションの対象とされている場合にはリボークされ、処理が終了する。若し、ホスト１０３がリボケーションの対象とされていなければ、ステップＳＴ２３において、コマンドSEND KEYにより、ドライブ１０２に対して乱数発生器１３６および１３７でそれぞれ生成された乱数Rb1と乱数Rb2を転送する。若し、ドライブ１０２がリボケーションの対象とされていなければ、ステップＳＴ１３において、ドライブ１０２がホスト１０3から転送されたこれらの乱数を受け取る。

【００７１】

その後、ホスト１０３は、コマンドREPORT KEYによりドライブ１０２に対してドライブ１０２が持つメディアキーＫｍを鍵としたＭＡＣによるレスポンス値と乱数生成器１２６が発生した乱数Ralとをホスト１０３へ転送することを要求する（ステップＳＴ２４）。このレスポンス値は、eKm(Ral‖Rbl)と表記される。ｅＫｍ（）は、メディアキーＫｍを暗号鍵として括弧内のデータを暗号化することを表している。Ral‖Rblの記号は、左側に乱数Ralを配し、右側に乱数Rblを配するように、二つの乱数を結合することを表している。

【００７２】

ホスト１０３からコマンドREPORT KEYを受け取ったドライブ１０２は、ステップＳＴ１４において、ＭＡＣ演算ブロック１２３が生成したＭＡＣ値eKm(Ral‖Rbl)と乱数Ralをホスト１０３へ転送する。ステップＳＴ２５において、ホスト１０３は、自身のＭＡＣ演算ブロック１３３でＭＡＣ値を計算し、比較１３９においてドライブ１０２から受け取った値と一致するかの確認を行う。若し、受け取ったＭＡＣ値と計算されたＭＡＣ値とが一致したのなら、ホスト１０３によるドライブ１０２の認証が成功したことになる。ステップＳＴ２５における比較の結果が同一でない場合には、ホスト１０３によるドライブ１０２の認証が失敗したことになり、リジェクト処理がなされる。

【００７３】

ホスト１０３によるドライブ１０２の認証が成功した場合には、ステップＳＴ

２６において、ホスト１０３がドライブ１０２へコマンドREPORT KEYを送付し、ドライブ１０２の乱数生成器１２４および１２５がそれぞれ生成する乱数Ｒa2と乱数Ｒa3の転送を要求する。このコマンドに応答して、ステップＳＴ１５において、ドライブ１０２は、これらの乱数をホスト１０３へ転送する。

【００７４】

ステップＳＴ２７において、ホスト１０３のＭＡＣ演算ブロック１３４は、ドライブ１０２から受け取った乱数からホスト１０３が持つメディアキーＫｍを鍵としたＭＡＣによるレスポンス値eKm(Rb2‖Ra2)を計算し、乱数Ｒb3とともに、コマンドSEND KEYを用いてドライブ１０２へ転送する。

【００７５】

ステップＳＴ１６において、ドライブ１０２は、ホスト１０３からレスポンス値eKm(Rb2‖Ra2)および乱数Rb3を受け取ると、自身でＭＡＣ値を計算し、ステップＳＴ１７において、比較１２９によってホスト１０３から受け取ったＭＡＣ値と一致するかの確認を行う。若し、受け取ったＭＡＣ値と計算されたＭＡＣ値とが一致したのなら、ドライブ１０２によるホスト１０３の認証が成功したことになる。この場合には、ステップＳＴ１８において、ＭＡＣ演算ブロック１２５がセッションキーeKm(Ra3‖Rb3)を生成し、また、ホスト１０３に対して認証が成功したことを示す情報を送信し、認証処理が完了する。セッションキーは、認証動作の度に異なる値となる。

【００７６】

ステップＳＴ１７における比較の結果が同一でない場合には、ドライブ１０２によるホスト１０３の認証が失敗したことになり、ステップＳＴ１９において、認証が失敗したことを示すエラー情報がホスト１０３に送信される。

【００７７】

ホスト１０３は、送付したコマンドSEND KEYに対する応答としてドライブ１０２から認証が成功したか否かを示す情報を受け取り、受け取った情報に基づいてステップＳＴ２８において、認証完了か否かを判断する。認証が成功したことを示す情報を受け取ることで認証完了と判断し、認証が失敗したことを示す情報を受け取ることで認証が完了しなかったと判断する。認証が完了した場合は、ステ

ップＳＴ２９において、ＭＡＣ演算ブロック１３５がドライブ側と共通のセッションキーeKm(Ra3‖Rb3)（例えば６４ビット長）を生成する。認証が完了しなかった場合には、リジェクト処理がなされる。セッションキーeKm(Ra3‖Rb3)を以下の説明では、適宜Ｋｓと表記する。

【００７８】

上述した一実施形態による相互認証は、ドライブ１０２がリボケーション機能を持つことができ、また、認証専用の特定の認証鍵を必要としない特徴を有している。

【００７９】

さらに、ドライブ１０２が比較１２９によってホスト１０３の認証結果を確認することで、ドライブ１０２がホスト１０３から正規のライセンスを受けた上で実装されたものであるか否かを判定することが可能となる。

【００８０】

次に、上述した相互認証を行うドライブ１０２とホスト１０３とを組み合わせて実現したレコーダの一実施形態の構成を図８に示す。一実施形態のレコーダは、ドライブ１０２が計算したメディアユニークキーを相互認証によって生成したセッションキーＫｓを用いてセキュアにホスト１０３に転送する。また、ドライブ１０２の乱数発生器１４３によってタイトルキーが生成される。ドライブ１０２においてタイトルキーおよびＣＣＩからコンテンツキーが生成され、生成されたコンテンツキーがセッションキーＫｓを用いてホスト１０３へセキュアに転送され、ホスト１０３が復号したコンテンツキーを用いてコンテンツを暗号化し、暗号化コンテンツをドライブ１０２へ転送し、ドライブ１０２が暗号化コンテンツ、暗号化タイトルキーおよびＣＣＩをメディア１０１へ記録する構成とされている。すなわち、ドライブ１０２において、メディアユニークキーおよびコンテンツキーを生成している。

【００８１】

レコーダを構成するドライブ１０２は、デバイスキー１２１、プロセスＭＫＢ１２２、Ｃ２＿Ｇ２１４１、ＤＥＳ(Data Encryption Standard)エンクリプタ１４２、乱数発生器１４３、Ｃ２＿Ｇ１４５、ＤＥＳエンクリプタ１４６の構成要

素を有する。Ｃ２＿Ｇ２１４１は、メディアＩＤとメディアキーからメディアユニークキーを演算するブロックである。Ｃ２＿Ｇ２１４５は、タイトルキーとＣＣＩとからコンテンツキーを演算するブロックである。

【００８２】

メディア１０１から再生されたＭＫＢ１１２とデバイスキー１２１とがプロセスＭＫＢ１２２において演算されることによって、リボケーションされたかどうかの判別ができる。プロセスＭＫＢ１２２において、ＭＫＢ１１２とデバイスキー１２１からメディアキーが算出される。ＭＫＢ１１２の中にドライブ１０２のデバイスキー１２１が入っておらず、演算された結果が予め決められたある値例えばゼロの値と一致した場合、そのデバイスキー１２１を持つドライブ１０２が正当なものでないと判断され、ドライブ１０２がリボケーションされる。

【００８３】

Ｃ２＿Ｇ１４１は、メディアキーとメディアＩＤ１１１とを演算し、メディアユニークキーを導出する処理である。メディアユニークキーがＤＥＳエンクリプタ１４２にてセッションキーＫｓによって暗号化される。暗号化の方式として、例えばＤＥＳ　ＣＢＣモードが使用される。ＤＥＳエンクリプタ１４２の出力がホスト１０３のＤＥＳデクリプタ１５１に送信される。

【００８４】

ドライブ１０２の乱数発生器１４３によってタイトルキーが生成され、乱数発生器１４３からのタイトルキーがホスト１０３のＣ２＿Ｅ１５３に供給され、タイトルキーがメディアユニークキーを使用してＣ２によって暗号化される。暗号化タイトルキー１１４がメディア１０１に記録される。

【００８５】

ホスト１０３において、セッションキーＫｓを鍵としてＭＡＣ演算ブロック１５８によりＣＣＩのＭＡＣ値ｅＫｓ（ＣＣＩ）が計算され、ＣＣＩとともにドライブ１０２へ転送される。

【００８６】

ドライブ１０２において、ホスト１０３から受け取ったＣＣＩからセッションキーＫｓを鍵としてＭＡＣ演算ブロック１５７によりＣＣＩのＭＡＣ値ｅＫｓ（

ＣＣＩ）が計算され、ホスト１０３から受け取ったＭＡＣ値とともに比較１５９へ供給される。

【００８７】

比較１５９では、両方のＭＡＣ値が一致したならば、ホスト１０３から受け取ったＣＣＩの改ざんは無いものと判断し、スイッチＳＷ２をＯＮする。一致しなかった場合は、ＣＣＩは改ざんされたものとみなし、スイッチＳＷ２をＯＦＦし、以降の処理を中断する。

【００８８】

ドライブ１０２において、ホスト１０３から受け取ったＣＣＩとタイトルキーとがＣ２＿Ｇ１４５に供給され、コンテンツキーが導出される。コンテンツキーがＤＥＳエンクリプタ１４６に供給され、セッションキーＫｓを鍵として、コンテンツキーが暗号化される。暗号化コンテンツキーがホスト１０３のＤＥＳデクリプタ１５６に転送される。

【００８９】

ホスト１０３のＤＥＳデクリプタ１５６でセッションキーＫｓを鍵として復号されたコンテンツキーがＣ２＿ＥＣＢＣ１５５に供給され、コンテンツキーを鍵としてコンテンツが暗号化される。暗号化コンテンツ１１３がドライブ１０２に転送され、ドライブ１０２によってメディア１０１に記録される。

【００９０】

図９は、レコーダの一実施形態によるコンテンツ記録時の手順を示すものである。最初に、ホスト１０３からの要求に応じてメディア１０１上のＭＫＢがシークされ、読み出される（ステップＳ６１）。次のステップＳ６２のＡＫＥ(Authentication and Key Exchange)において、上述したようなリボーク処理とドライブ１０２とホスト１０３の相互認証動作がなされる。

【００９１】

相互認証動作は、電源のＯＮ後のディスク検出時並びにディスクの交換時には、必ず行われる。また、記録ボタンを押して記録動作を行う場合、並びに再生ボタンを押して再生動作を行う場合に、認証動作を行うようにしても良い。一例として、記録ボタンまたは再生ボタンを押した時に、認証がなされる。

【００９２】

相互認証が成功しないと、リジェクト処理によって例えば処理が中断する。相互認証が成功すると、ドライブ１０２およびホスト１０３の両者において、セッションキーＫｓが生成され、セッションキーＫｓが共有される。

【００９３】

次のステップＳ６３において、ホスト１０３がドライブ１０２に対してメディアユニークキーを要求する。ドライブ１０２は、メディア１０１のメディアＩＤをシークし（ステップＳ６４）、メディアＩＤをメディア１０１から読み出す（ステップＳ６５）。ドライブ１０２は、メディアキーとメディアＩＤとを演算することによってメディアユニークキーを生成する。ステップＳ６６において、メディアユニークキーがセッションキーＫｓによって暗号化され、暗号化されたメディアユニークキーがホスト１０３に転送される。

【００９４】

次に、ステップＳ６７において、ホスト１０３がドライブ１０２に対してタイトルキーを要求する。ステップＳ６８において、ドライブ１０２がタイトルキーをホスト１０３に転送する。ホスト１０３において、セッションキーＫｓによって、暗号化されたメディアユニークキーが復号される。そして、タイトルキーがメディアユニークキーによって暗号化され、暗号化タイトルキーが生成される。

【００９５】

また、ステップＳ６９において、ホスト１０３がドライブ１０２に対してＣＣＩを送る。このとき、ＣＣＩの改ざんを回避するためにＣＣＩの認証データとして計算されたＭＡＣ値ｅＫｓ（ＣＣＩ）を付加して転送する。ドライブ１０２において、ＣＣＩの改ざんが無いことを確認後、タイトルキーとＣＣＩからコンテンツキーが生成され、コンテンツキーがセッションキーＫｓで暗号化される。ステップＳ７０において、ホスト１０３がドライブ１０２に対してコンテンツキーを要求すると、ステップＳ７１において、ドライブ１０２が暗号化されたコンテンツキーをホスト１０３に送る。

【００９６】

ホスト１０３は、暗号化コンテンツキーをセッションキーＫｓによって復号し

、コンテンツキーを得る。コンテンツキーによってコンテンツが暗号化される。ステップＳ７２において、ホスト１０３からドライブ１０２に対して、暗号化タイトルキー、暗号化コンテンツおよびＣＣＩが転送される。ステップＳ７３において、ドライブ１０２によって、暗号化タイトルキー、暗号化コンテンツおよびＣＣＩがメディア１０１に対して記録される。

【００９７】

上述した図８に示す構成のレコーダは、ドライブ１０２において、真正乱数またはそれに近い乱数をハードウエア例えばＬＳＩによって発生することができ、生成した乱数を固定値への置き換えを困難とすることができる。また、ドライブ１０２において、ハードウエア構成によってコンテンツキーを生成するので、著作権保護の実装を強力とすることができる。

【００９８】

次に、上述した相互認証を行うドライブ１０２とホスト１０３とを組み合わせて実現したプレーヤの一実施形態の構成を図１０に示す。一実施形態のプレーヤは、ドライブ１０２が計算したメディアユニークキーを相互認証によって生成したセッションキーＫｓを用いてセキュアにホスト１０３に転送し、ホスト１０３が暗号化タイトルキーをメディアユニークキーによって復号し、タイトルキーとＣＣＩとから導出したコンテンツキーを用いてコンテンツを復号する構成とされている。

【００９９】

プレーヤを構成するドライブ１０２は、デバイスキー１２１、プロセスＭＫＢ１２２、Ｃ２＿Ｇ２１４１、ＤＥＳエンクリプタ１４２の構成要素を有する。メディア１０１から再生されたＭＫＢ１１２とデバイスキー１２１とがプロセスＭＫＢ１２２において演算されることによって、リボケーションされたかどうかの判別ができる。プロセスＭＫＢ１２２において、ＭＫＢ１１２とデバイスキー１２１からメディアキーが算出される。

【０１００】

Ｃ２＿Ｇ１４１は、メディアキーとメディアＩＤ１１１とを演算し、メディアユニークキーを導出する処理である。メディアユニークキーがＤＥＳエンクリプ

タ１４２にてセッションキーＫｓによって暗号化される。暗号化の方式として、例えばＤＥＳ　ＣＢＣモードが使用される。ＤＥＳエンクリプタ１４２の出力がホスト１０３のＤＥＳデクリプタ１５１に送信される。

【０１０１】

ホスト１０３において、ＤＥＳデクリプタ１５１において、セッションキーＫｓによってメディアユニークキーが復号される。メディアユニークキーおよび暗号化タイトルキー１１４がＣ２＿Ｄ１５３に供給され、暗号化タイトルキーがメディアユニークキーを使用して復号される。復号されたタイトルキーとメディア１０１から再生されたＣＣＩがＣ２＿Ｇ１５４に供給され、コンテンツキーが導出される。メディア１０１から再生された暗号化コンテンツ１１３がＣ２デクリプタ１５５において、コンテンツキーによって復号され、コンテンツキーが得られる。

【０１０２】

図１１は、コンテンツ再生時の手順を示すものである。最初に、ホスト１０３からの要求に応じてメディア１０１上のＭＫＢがシークされ、読み出される（ステップＳ４１）。ＭＫＢがパック毎に読み出される。次のステップＳ４２のＡＫＥにおいて、上述したようなリボーク処理と、ドライブ１０２とホスト１０３の相互認証動作がなされる。

【０１０３】

相互認証が成功しないと、リジェクト処理によって例えば処理が中断する。相互認証が成功すると、ドライブ１０２およびホスト１０３の両者において、セッションキーＫｓが生成され、セッションキーＫｓが共有される。

【０１０４】

次のステップＳ４３において、ホスト１０３がドライブ１０２に対してメディアユニークキーを要求する。ドライブ１０２は、メディア１０１のメディアＩＤをシークし（ステップＳ４４）、メディアＩＤをメディア１０１から読み出す（ステップＳ４５）。ドライブ１０２は、メディアキーとメディアＩＤとを演算することによってメディアユニークキーを生成する。ステップＳ４６において、メディアユニークキーがセッションキーＫｓによって暗号化され、暗号化されたメ

ディアユニークキーがホスト１０３に転送される。

【０１０５】

次に、ステップＳ４７において、ホスト１０３がドライブ１０２に対して、暗号化タイトルキー、ＣＣＩおよび暗号化コンテンツを要求する。ステップＳ４８において、ドライブ１０２が暗号化タイトルキー１１４、ＣＣＩ１１５および暗号化コンテンツ１１３をメディア１０１からリードする。ステップＳ４９において、ドライブ１０２が暗号化タイトルキー１１４、ＣＣＩ１１５および暗号化コンテンツ１１３を読み取る。そして、ステップＳ５０において、ドライブ１０２が暗号化タイトルキー１１４、ＣＣＩ１１５および暗号化コンテンツ１１３をホスト１０３に対して転送する。

【０１０６】

ホスト１０３において、タイトルキーが復号され、タイトルキーとＣＣＩとからコンテンツキーが求められ、コンテンツキーを鍵として暗号化コンテンツが復号される。

【０１０７】

図１０に示すプレーヤの構成においては、ホスト１０３が暗号化タイトルキーを復号するデクリプタＣ２＿Ｄ１５３を備えているが、ドライブ１０２が暗号化タイトルキーを復号するデクリプタを備えるようにしても良い。この場合、復号されたタイトルキーがホスト１０３のコンテンツキー生成用のＣ２＿Ｇ１５４に対してセキュアに転送される。または、ドライブ１０２にコンテンツキー生成装置Ｃ２＿Ｇを設け、ドライブ１０２において復号されたタイトルキーとＣＣＩとからコンテンツキーを生成するようにしても良い。この場合、復号されたコンテンツキーがホスト１０３のＣ２＿ＤＣＢＣ１５５へセキュアに転送される。

【０１０８】

この発明は、上述したこの発明の一実施形態等に限定されるものではなく、この発明の要旨を逸脱しない範囲内で様々な変形や応用が可能である。例えばタイトルキーは、タイトル毎のキーであるが、この発明では、乱数情報であれば、タイトル毎に異なることは、必要ではない。

【０１０９】

また、上述した説明においては、著作権保護技術としてＣＰＲＭおよびＣＰＲＭを拡張した例を挙げたが、ＣＰＲＭ以外の著作権保護技術に対してもこの発明を適用することができる。例えば、特開2001－352322号公報において提案されるツリー構造の鍵配布構成に基づく著作権保護技術に対して適用可能である。また、ＰＣベースのシステムに対してこの発明が適用されるが、このことは、ＰＣとドライブを組み合わせる構成にのみ限定されることを意味するものではない。例えば携帯型動画または静止画カメラの場合に、メディアとして光ディスクを使用し、メディアを駆動するドライブとドライブを制御するマイクロコンピュータが設けられる動画または静止画カメラシステムに対してもこの発明を適用することが可能である。

【０１１０】

【発明の効果】

この発明では、再生装置側でコンテンツキーを生成し、コンテンツキーを情報処理装置へ送信し、情報処理装置側でコンテンツキーによってコンテンツを暗号化している。このように著作権保護のための鍵情報の生成を再生装置で行うので、ハードウエア構成でコンテンツキーを生成することが可能となり、耐タンパー性を高めることができる。また、再生装置において、乱数を生成し、乱数を中間鍵とするので、再生装置において、真正乱数またはそれに近い乱数をハードウエア例えばＬＳＩによって発生することができ、生成した乱数を固定値への置き換えを困難とすることができる。このように、この発明では、情報処理装置にインストールされるアプリケーションソフトウェアは、著作権保護技術に関する秘密情報の全てを持つ必要がなくなる。それによって、ソフトウェアのリバースエンジニアリングによる解析に対する耐性を持たせることが容易に実施でき、また、ディスクからのデータとしてそのまま読み出された暗号化コンテンツが「ＤｅＣＳＳ」のような解読ソフトウェアにより復号され、平文のままのクリア・コンテンツとしてコピー制限の働かない状態で複製が繰り返されるような事態を防ぐことができることから、著作権保護技術の安全性を確保することができる。

【０１１１】

また、電子機器固有の情報としてのデバイスキーを記録再生装置が持つことに

よって、記録再生装置自身をリボークすることが可能となる。さらに、この発明では、情報処理装置におけるコンテンツキーを計算するのに必要とされる乱数情報が記録再生装置内の例えばＬＳＩによって生成できるので、ＰＣ内でソフトウェアによって乱数を生成するのと比較して、真正または真正乱数に近い乱数を生成することができる。したがって、乱数が固定値に置き換えられる、等のおそれを少なくできる。

【図面の簡単な説明】

【図１】

先に提案されているレコーダ、プレーヤおよびＤＶＤメディアからなるシステムを説明するためのブロック図である。

【図２】

ＰＣベースのＤＶＤメディア記録再生システムを説明するためのブロック図である。

【図３】

図２のシステムにおけるＤＶＤドライブ４およびホスト５の処理の手順を説明するための略線図である。

【図４】

図２のシステムにおける認証動作を説明するためのフローチャートである。

【図５】

この発明の一実施形態による相互認証のための構成を示すブロック図である。

【図６】

この発明の一実施形態におけるドライブの認証動作の処理の手順を説明するためのフローチャートである。

【図７】

この発明の一実施形態におけるホストの認証動作の処理の手順を説明するためのフローチャートである。

【図８】

この発明の一実施形態によるドライブとホストを組み合わせたレコーダの構成の一例をブロック図である。

【図９】

レコーダの一例の通信の手順を説明するための略線図である。

【図１０】

この発明の一実施形態によるドライブとホストを組み合わせたプレーヤの構成の一例をブロック図である。

【図１１】

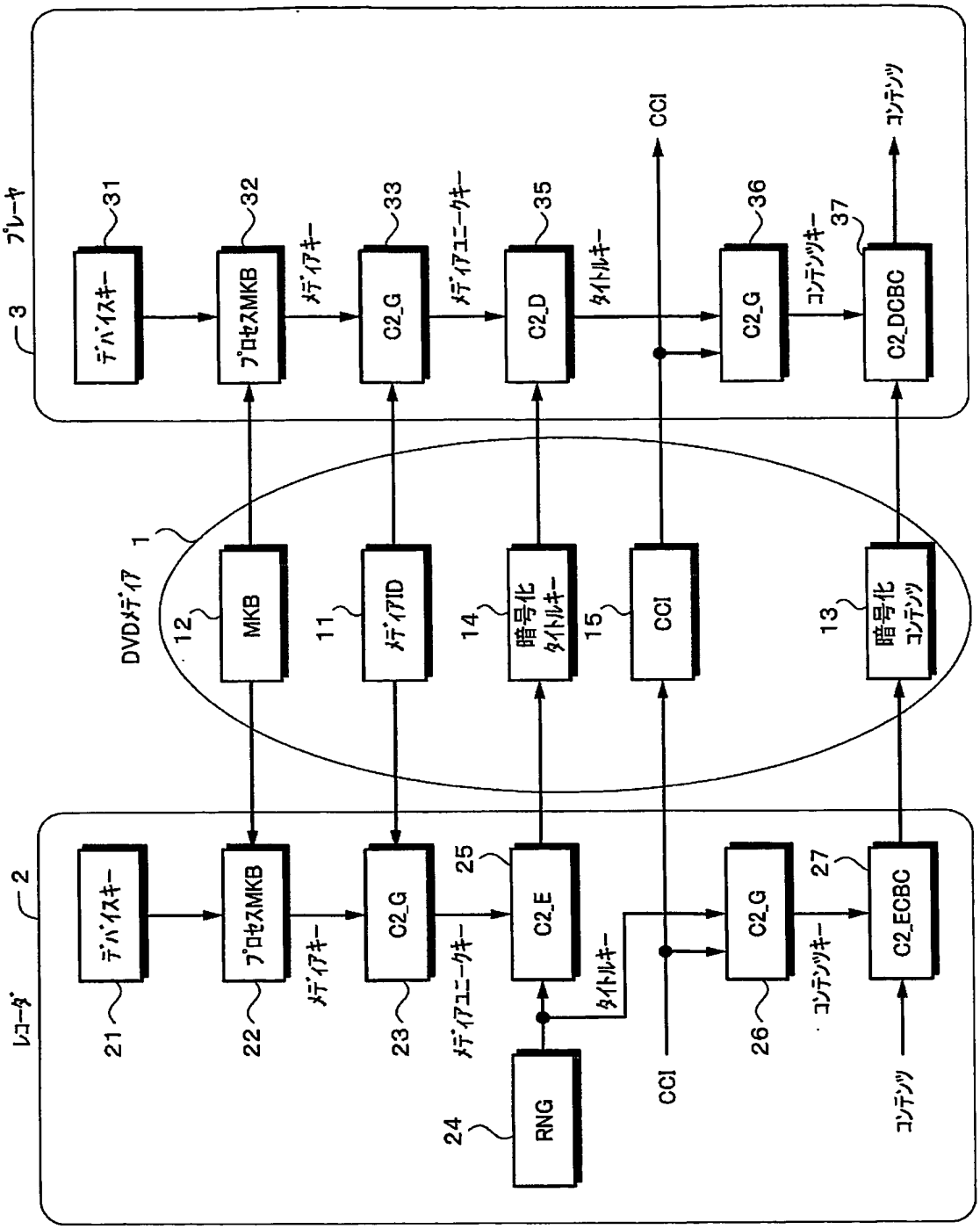
プレーヤの一例の通信の手順を説明するための略線図である。

【符号の説明】

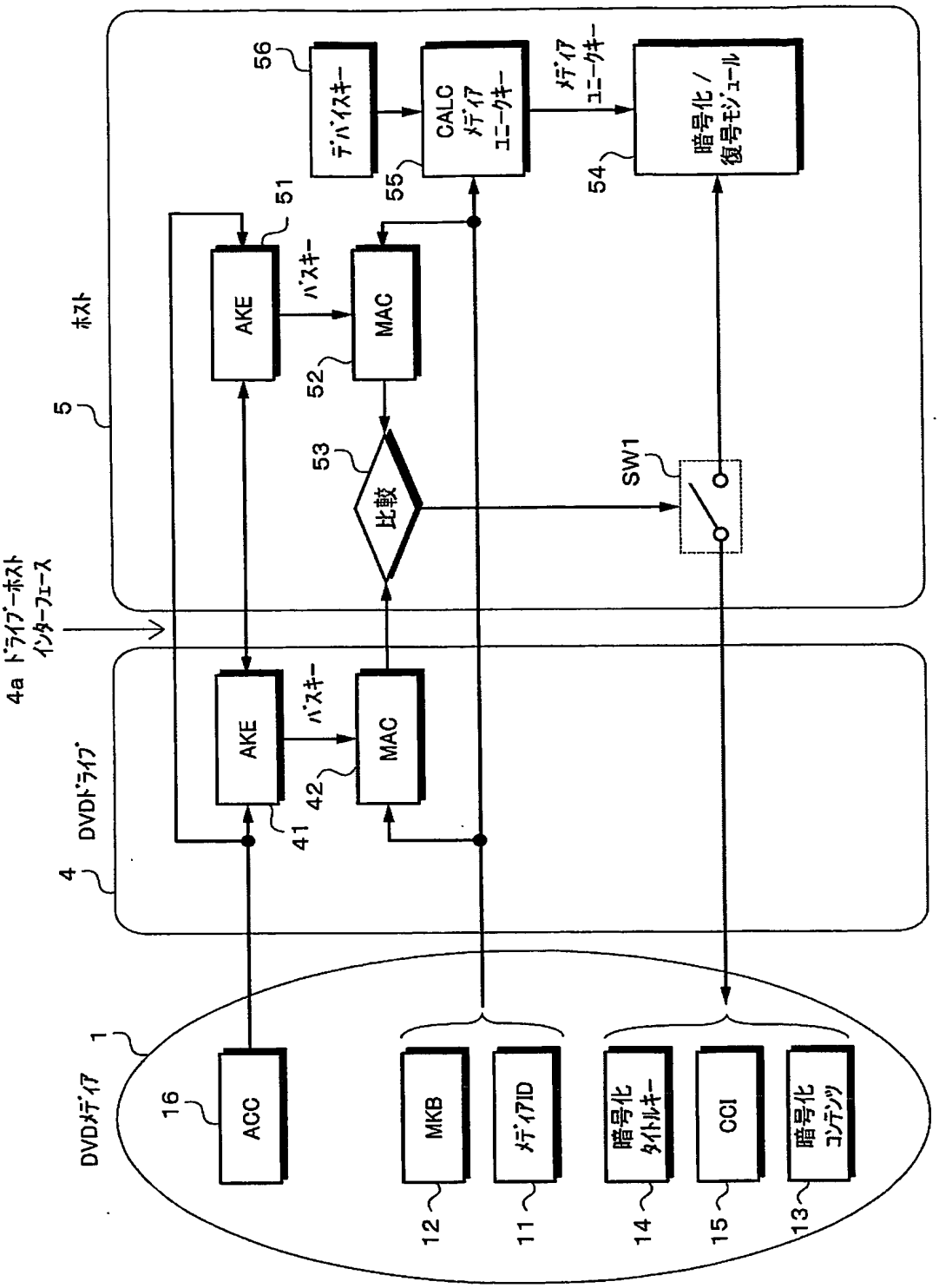
１・・・ＤＶＤメディア、２・・・レコーダ、３・・・プレーヤ、４・・・ＤＶＤドライブ、４ａ・・・インターフェース、５・・・ホスト、１１・・・メディアＩＤ、１２・・・メディアキーブロック（ＭＫＢ）、１３・・・暗号化コンテンツ、４２，５２・・・ＭＡＣ演算ブロック、４６・・・デバイスキー、４６ａ・・・デバイスキーの前半部、４７・・・ＤＥＳエンクリプタ、４８・・・メディアユニークキー演算ブロック、４９，４９ａ・・・ＤＥＳエンクリプタ、４９ｂ・・・ＤＥＳデクリプタ、５３・・・ＭＡＣを比較する比較、５４・・・暗号化／復号モジュール、５５・・・メディアユニークキー演算ブロック、１０１・・・メディア、１０２・・・ドライブ、１０３・・・ホスト、１０４・・・インターフェース、１２１・・・ドライブのデバイスキー、１２２・・・プロセスＭＫＢ、１２３，１２４，１２５・・・ドライブのＭＡＣ演算ブロック、１２６，１２７，１２８・・・ドライブの乱数発生器、１２９・・・比較、１３１・・・ホストのデバイスキー、１３２・・・プロセスＭＫＢ、１３３，１３４，１３５・・・ホストのＭＡＣ演算ブロック、１３６，１３７，１３８・・・ホストの乱数発生器、１３９・・・比較、１４１，１５４・・・Ｃ２＿Ｇ、１４２・・・ＤＥＳエンクリプタ、１４３・・・乱数発生器、１５１，１５６・・・ＤＥＳデクリプタ、１５３・・・Ｃ２＿Ｅ、１５５・・・Ｃ２＿ＥＢＣ、１５７，１５８・・・ＭＡＣ演算ブロック、１５９・・・比較

【書類名】　図面

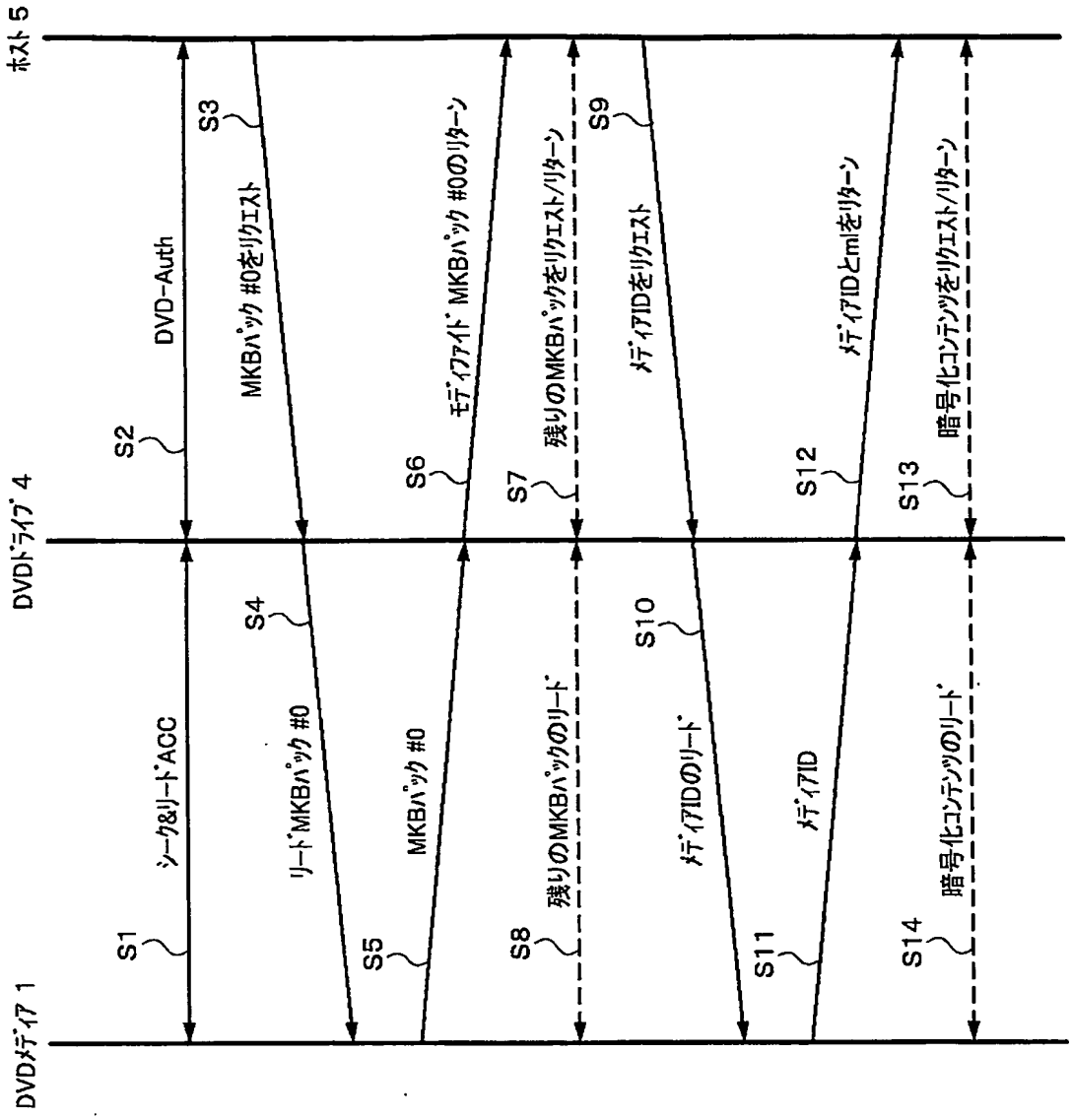
【図１】


プレーヤ
3
デバイスキー
31
プロセスMKB
32
メディアキー
C2_G
33
メディアユニークキー
C2_D
35
タイトルキー
CCI
C2_G
36
コンテンツキー
37
C2_DCBC
コンテンツ
DVDメディア
1
MKB
12
メディアID
11
暗号化タイトルキー
14
CCI
15
暗号化コンテンツ
13
レコーダ
2
デバイスキー
21
プロセスMKB
22
メディアキー
C2_G
23
メディアユニークキー
25
C2_E
タイトルキー
RNG
24
CCI
C2_G
26
コンテンツキー
27
C2_ECBC
コンテンツ

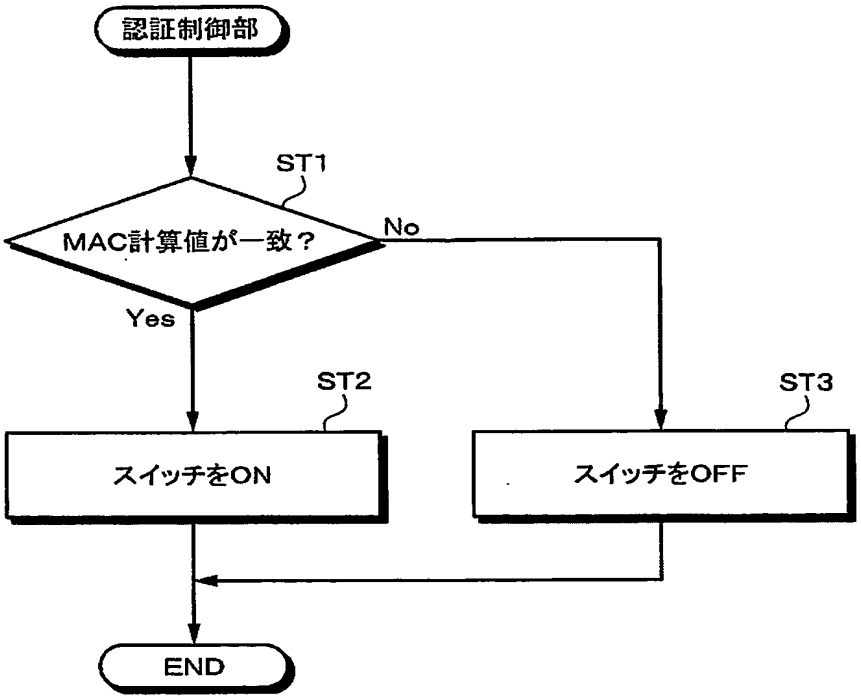
【図２】


DVDメディア
1
16
ACC
MKB
12
メディアID
11
暗号化タイトルキー
14
CCI
15
暗号化コンテンツ
13
4
DVDドライブ
41
AKE
バスキー
42
MAC
4a ドライブ－ホスト インターフェース
5
ホスト
51
AKE
バスキー
52
MAC
53
比較
SW1
54
暗号化／復号モジュール
メディアユニークキー
55
CALC メディアユニークキー
56
デバイスキー

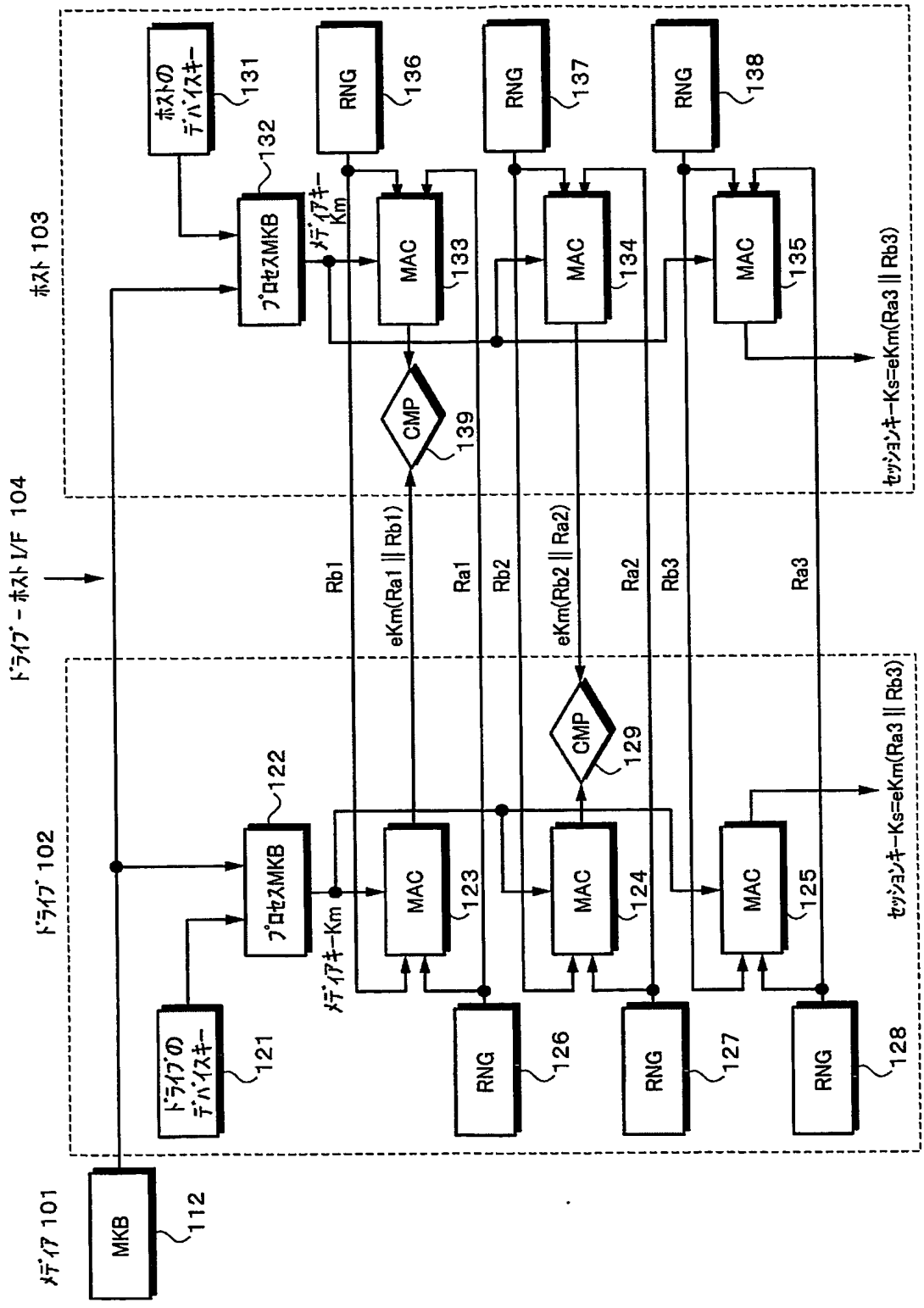
【図３】


ホスト 5
DVDドライブ 4
DVDメディア 1
S1
シーク&リードACC
S2
DVD-Auth
S3
MKBパック #0をリクエスト
S4
リードMKBパック #0
S5
MKBパック #0
S6
モディファイドMKBパック #0のリターン
S7
残りのMKBパックをリクエスト/リターン
S8
残りのMKBパックのリード
S9
メディアIDをリクエスト
S10
メディアIDのリード
S11
メディアID
S12
メディアIDとmlをリターン
S13
暗号化コンテンツをリクエスト/リターン
S14
暗号化コンテンツのリード

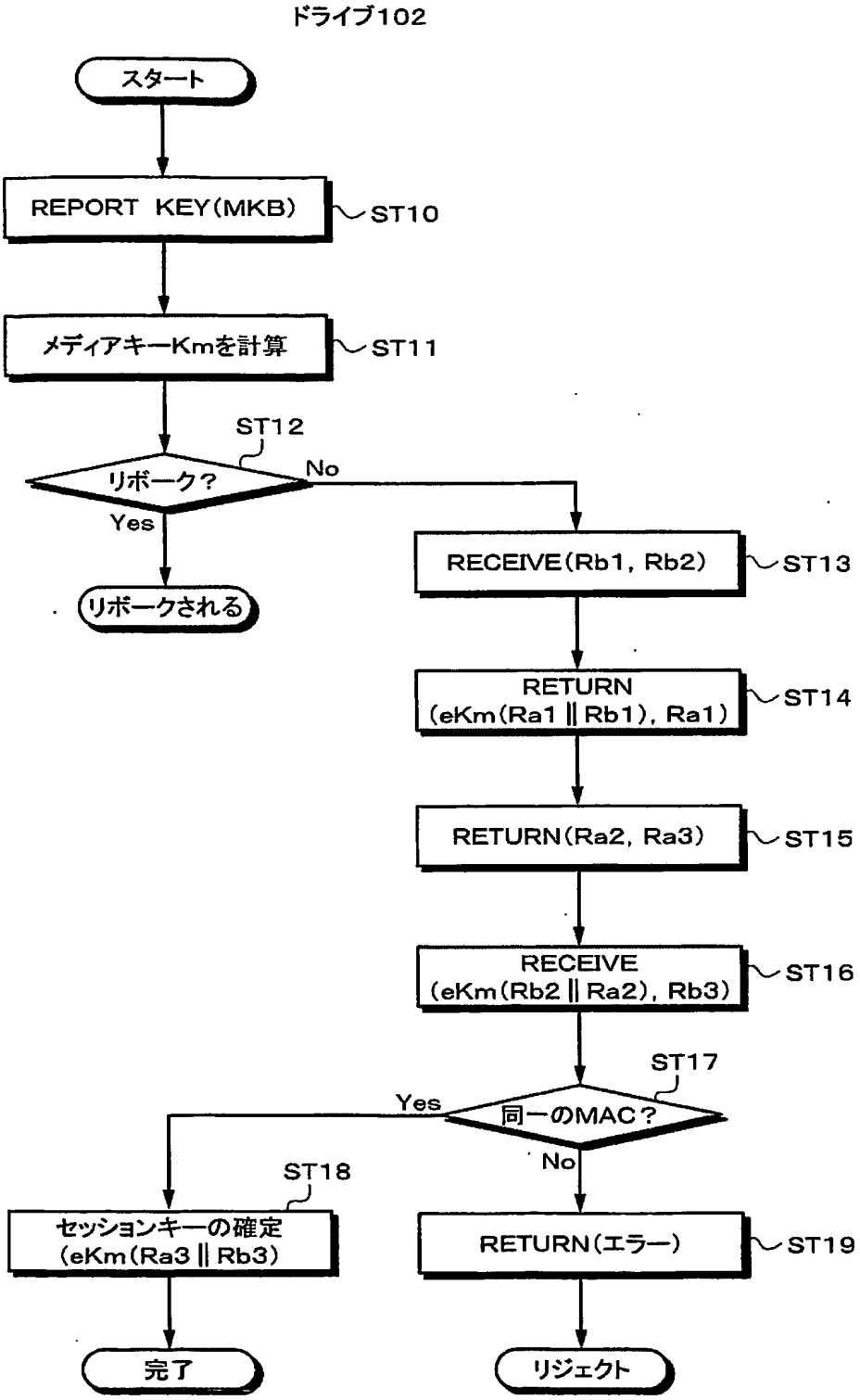
【図４】



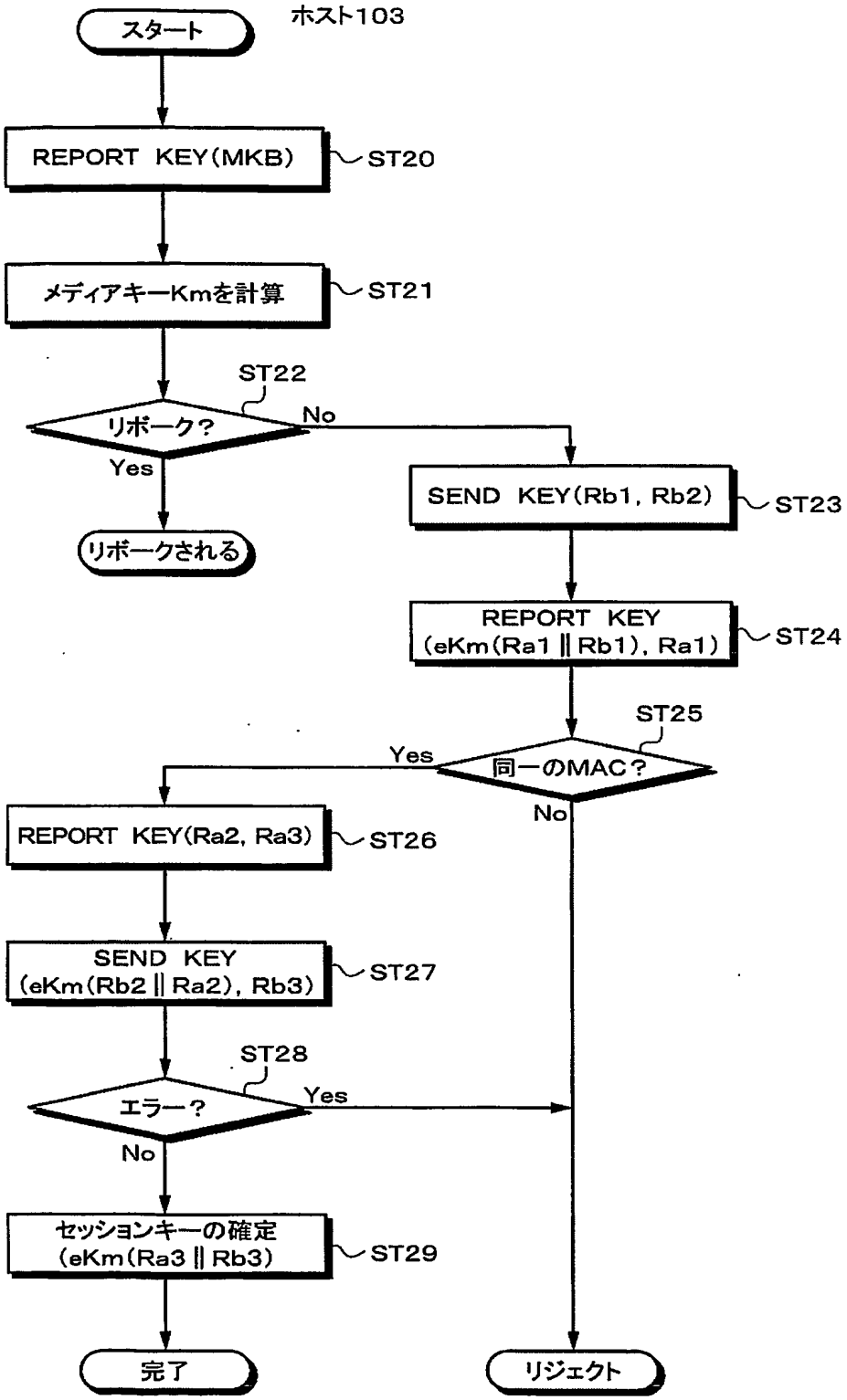
【図５】


ホスト 103
ドライブ－ホストI/F 104
ドライブ 102
メディア 101
ホストのデバイスキー
131
132
プロセスMKB
メディアキーKm
MAC
133
MAC
134
MAC
135
RNG
136
RNG
137
RNG
138
CMP
139
セッションキーKs=eKm(Ra3 || Rb3)
Rb1
eKm(Ra1 || Rb1)
Ra1
Rb2
eKm(Rb2 || Ra2)
Ra2
Rb3
Ra3
CMP
129
プロセスMKB
122
メディアキーKm
MAC
123
MAC
124
MAC
125
セッションキーKs=eKm(Ra3 || Rb3)
ドライブのデバイスキー
121
RNG
126
RNG
127
RNG
128
MKB
112

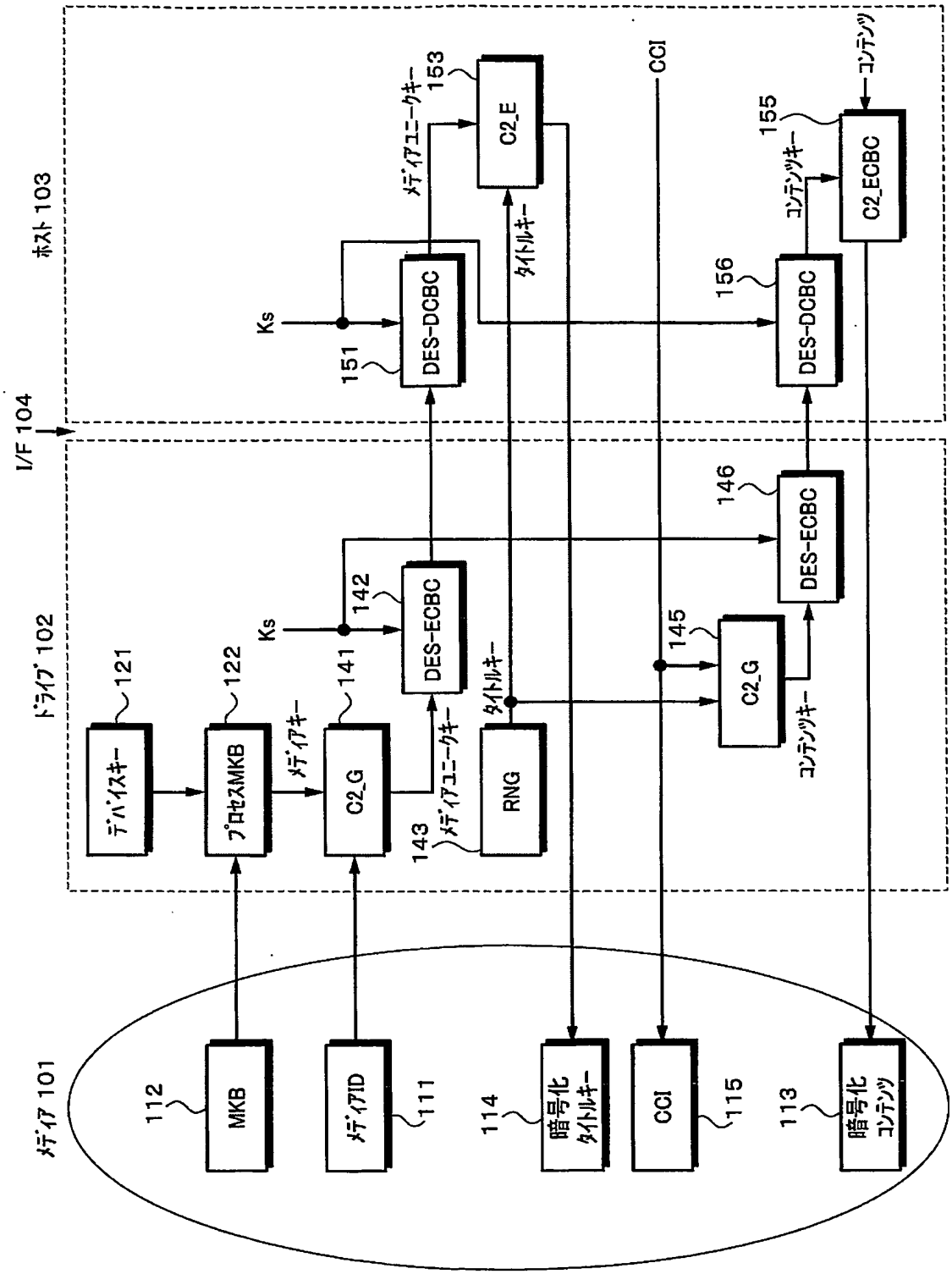
【図６】


ドライブ102
スタート
REPORT KEY(MKB)
ST10
メディアキーKmを計算
ST11
ST12
リボーク？
No
Yes
リボークされる
RECEIVE(Rb1, Rb2)
ST13
RETURN
(eKm(Ra1 ‖ Rb1), Ra1)
ST14
RETURN(Ra2, Ra3)
ST15
RECEIVE
(eKm(Rb2 ‖ Ra2), Rb3)
ST16
ST17
Yes
同一のMAC？
No
ST18
セッションキーの確定
(eKm(Ra3 ‖ Rb3)
RETURN(エラー)
ST19
完了
リジェクト

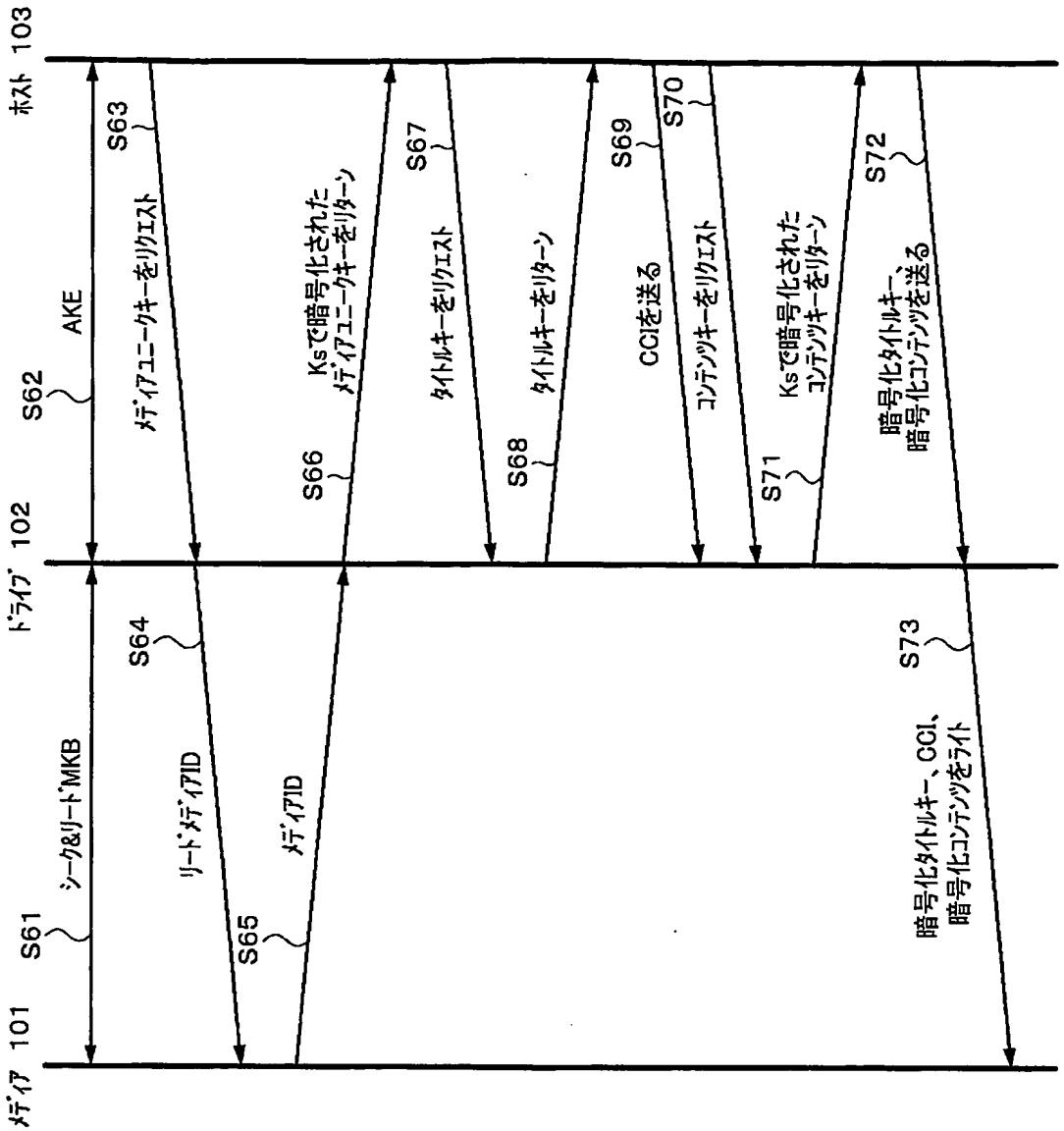
【図７】


スタート
ホスト103
REPORT KEY(MKB)
ST20
メディアキーKmを計算
ST21
ST22
リボーク？
No
Yes
リボークされる
SEND KEY(Rb1, Rb2)
ST23
REPORT KEY
(eKm(Ra1 ‖ Rb1), Ra1)
ST24
ST25
Yes
同一のMAC？
No
REPORT KEY(Ra2, Ra3)
ST26
SEND KEY
(eKm(Rb2 ‖ Ra2), Rb3)
ST27
ST28
エラー？
Yes
No
セッションキーの確定
(eKm(Ra3 ‖ Rb3)
ST29
完了
リジェクト

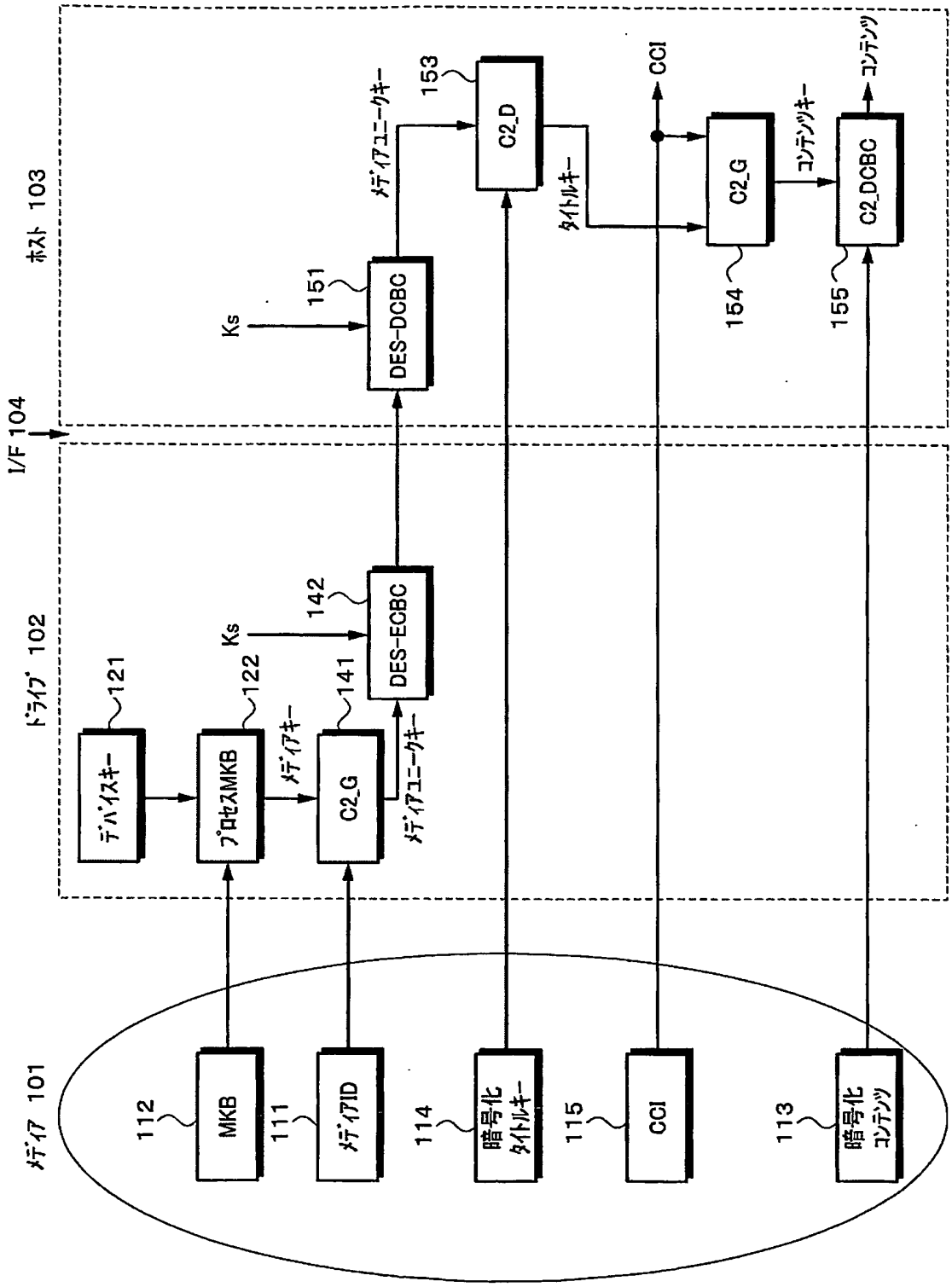
【図８】


ホスト 103
I/F 104
ドライブ 102
メディア 101
デバイスキー
121
プロセスMKB
122
メディアキー
C2_G
141
DES-ECBC
142
Ks
メディアユニークキー
143
RNG
タイトルキー
C2_G
145
DES-ECBC
146
コンテンツキー
DES-DCBC
151
Ks
メディアユニークキー
153
C2_E
タイトルキー
CCI
DES-DCBC
156
コンテンツキー
155
C2_ECBC
コンテンツ
MKB
112
メディアID
111
暗号化タイトルキー
114
CCI
115
暗号化コンテンツ
113

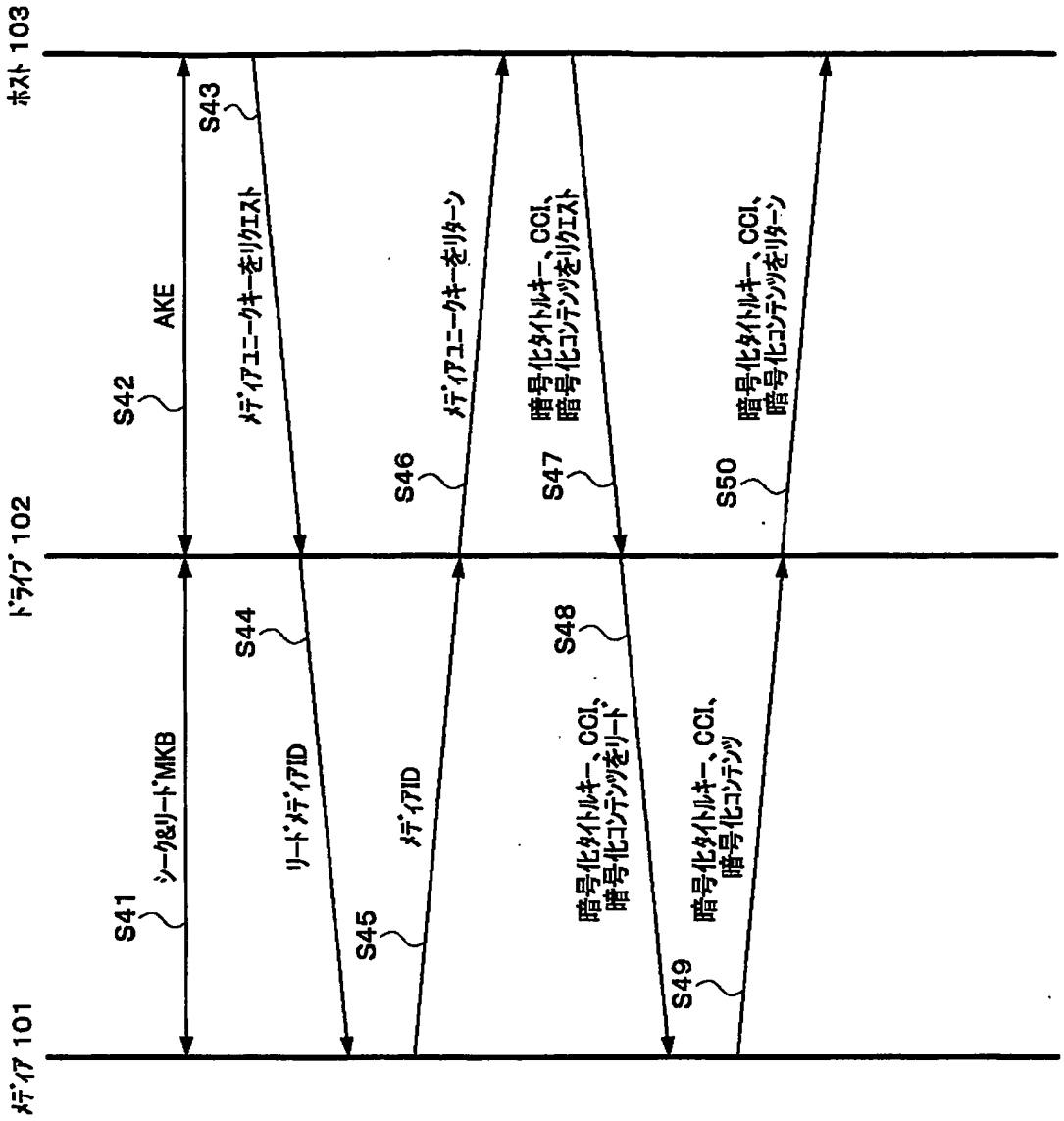
【図９】


ホスト 103
ドライブ 102
メディア 101
S61
シーク&リード'MKB
S62
AKE
S63
メディアユニークキーをリクエスト
S64
リード'メディアID
S65
メディアID
S66
Ksで暗号化されたメディアユニークキーをリターン
S67
タイトルキーをリクエスト
S68
タイトルキーをリターン
S69
CCIを送る
S70
コンテンツキーをリクエスト
S71
Ksで暗号化されたコンテンツキーをリターン
S72
暗号化タイトルキー、暗号化コンテンツを送る
S73
暗号化タイトルキー、CCI、暗号化コンテンツをライト

【図１０】


メディア 101
ドライブ 102
ホスト 103
I/F 104
MKB
メディアID
暗号化タイトルキー
CCI
暗号化コンテンツ
デバイスキー
プロセスMKB
C2_G
DES-ECBC
DES-DCBC
C2_D
C2_G
C2_DCBC
Ks
メディアキー
メディアユニークキー
タイトルキー
コンテンツキー
コンテンツ
111
112
113
114
115
121
122
141
142
151
153
154
155

【図１１】


ホスト 103
ドライブ 102
メディア 101
S41
シーク&リード'MKB
S42
AKE
S43
メディアユニークキーをリクエスト
S44
リード'メディアID
S45
メディアID
S46
メディアユニークキーをリターン
S47
暗号化タイトルキー、CCI、暗号化コンテンツをリクエスト
S48
暗号化タイトルキー、CCI、暗号化コンテンツをリード
S49
暗号化タイトルキー、CCI、暗号化コンテンツ
S50
暗号化タイトルキー、CCI、暗号化コンテンツをリターン

【書類名】　要約書

【要約】

【課題】　著作権保護技術の安全性を確保する。

【解決手段】　相互認証を行うドライブ１０２とホスト１０３とからレコーダが構成される。ドライブ１０２のＣ２＿Ｇ２１４１がメディアＩＤとメディアキーから計算したメディアユニークキーが相互認証によって生成したセッションキーＫｓを用いて暗号化されてからホスト１０３に転送される。ドライブ１０２の乱数発生器１４３が発生したタイトルキーがホスト１０３に転送される。ドライブ１０２のＣ２＿Ｇ２１４５がタイトルキーとＣＣＩとから計算したコンテンツキーがセッションキーＫｓを用いて暗号化されてからホスト１０３へ転送される。ホスト１０３が復号したコンテンツキーを用いてコンテンツを暗号化し、ドライブ１０２が暗号化コンテンツ、暗号化タイトルキーおよびＣＣＩをメディア１０１へ記録する。

【選択図】　図８

出願人履歴情報

識別番号　［０００００２１８５］

１．変更年月日　１９９０年　８月３０日
［変更理由］　新規登録
住　所　東京都品川区北品川６丁目７番３５号
氏　名　ソニー株式会社